ALI/ELI

PRINCIPLES FOR A DATA ECONOMY

Data Transactions and Data Rights

As Adopted and Promulgated

BY

The American Law Institute
on
May 18, 2021

and The European Law Institute
on
September 1, 2021

Principles 1 to 40

THE AMERICAN LAW INSTITUTE AND THE EUROPEAN LAW INSTITUTE

2023

ALI REPORTERS, ADVISERS, AND LIAISON
Principles for a Data Economy

(as of April 26, 2021)

REPORTERS

NEIL B. COHEN, Brooklyn Law School, Brooklyn, NY
CHRISTIANE C. WENDEHORST, University of Vienna, Department of Civil Law, Vienna, Austria

CO-CHAIRS

LORD JOHN THOMAS OF CWMGIEDD, Essex Court Chambers, London, England
STEVEN O. WEISE, Proskauer Rose LLP, Bainbridge Island, WA

CONSULTANTS

ANUPAM CHANDER, Georgetown University Law Center, Washington, DC
CHRISTOPHER S. YOO, University of Pennsylvania Carey Law School, Philadelphia, PA

ADVISERS

SUSAN BENNETT, IRi, Chicago, IL
HANNAH BLOCH-WEHBA, Texas A&M University School of Law, Fort Worth, TX
AMELIA H. BOSS, Drexel University Thomas R. Kline School of Law, Philadelphia. PA
JULIE S. BRILL, Microsoft Corporation, Redmond, WA
SARAH C. DODDS-BROWN, American Express, New York, NY
STACY-ANN ELVY, University of California, Davis, School of Law, Davis, CA
LINDSEY FINCH, Salesforce.com, San Francisco, CA
IVAN K. FONG, 3M Co., St. Paul, MN
AHMED GHAPPOUR, Boston University School of Law, Boston, MA
JAMES GRIMMELMANN, Cornell Law School, New York, NY
ANTON G. HAJJAR, Chevy Chase, MD
TERESA WILTON HARMON, Sidley Austin, Chicago, IL
MICHELE C. KANE, The Walt Disney Company, Valley Village, CA
HAROLD HONGJU KOH, Yale Law School, New Haven, CT
LUCY H. KOH, U.S. District Court, Northern District of California, San Jose, CA
TRAVIS LEBLANC, Cooley, Washington, DC
HENRY LEBOWITZ, Debevoise & Plimpton, New York, NY
RONALD D. LEE, Arnold & Porter, Washington, DC
MICHAEL LEITER, Skadden, Arps, Slate, Meagher & Flom, Washington, DC
LANCE LIEBMAN, Columbia Law School, New York, NY
CHRISTINA MULLIGAN, Brooklyn Law School, Brooklyn, NY
STEPHEN SATTERFIELD, Facebook Inc., Washington, DC
CHRISTOPHER H. SCHROEDER, Duke University School of Law, Durham, NC
PAUL M. SCHWARTZ, University of California, Berkeley School of Law, Berkeley, CA
JEEWON K. SERRATO, BakerHostetler, San Francisco, CA
PETER P. SWIRE, Georgia Tech, Ernest Scheller Jr. College of Business, Atlanta, GA

LIAISON

For The American Bar Association Section of Intellectual Property Law
STEPHEN YEE CHOW, Boston, MA

ELI ADVISORY COMMITTEE

Principles for a Data Economy

(as of April 26, 2021)

BENOIT VAN ASBROECK, Bird & Bird, BE
JOSE ANTONIO CASTILLO PARRILLA, University of Granada, ES
PETER DONNELLY, University of Oxford, UK
JOSEF DREXL, Max Planck Institute for Innovation and Competition, DE
SJEF VAN ERP, Maastricht University, NL
BÉNÉDICTE FAUVARQUE-COSSON, Université Panthéon-Assas Paris II, FR
SIMON GEIREGAT, Ghent University, BE
ZOUBIN GHAHRAMANI, University of Cambridge; Uber, UK
FRIEDRICH GRAF VON WESTPHALEN, Graf von Westphalen, DE
VÁCLAV JANEČEK, Oxford University, Faculty of Law, CZ
JOSÉ CARMELO LLOPIS BENLLOCH, Ayora Valencia (Spain); Member of the Council of the Notariats of the European Union (CNUE), ES
AXEL METZGER, Humboldt University Berlin, DE
FRANCISCO MOLINA BALAGUER, Land Registrar in Lleida, ES
JOANNA PERKINS, London Financial Markets Law Committee, UK
PASCAL PICHONNAZ, University of Fribourg, CH
RADIM POLČÁK, Institute for Law and Technology, Masaryk University Brno, CZ
GILES PRATT, Freshfields Bruckhaus Deringer, UK
MARTIN SCHMIDT-KESSEL, University of Bayreuth, DE
JULIETTE SÉNÉCHAL, University Lille II, FR
SAM DE SILVA, CMS Cameron McKenna Nabbarao Olswang LLP; Nabbaro LLP, UK; NZ
GERALD SPINDLER, University of Göttingen, Faculty of Law, DE
ANA KEGLEVIĆ STEFFEK, Anglia Ruskin University, HR
ALAIN STROWEL, Université Saint-Louis Bruxelles, UCLouvain, BE
LOREDANA TASSONE, Alphalex (Brussels); Council of Europe, IT
CHRISTIAN TWIGG-FLESNER, University of Warwick, UK
JOS UITDEHAAG, International Union of Judicial Officers (UIHJ), NL
JACQUES DE WERRA, University of Geneva, CH
HERBERT ZECH, University of Basel, DE

ELI CONSULTANTS

YANNICK DULLER, University of Vienna, Vienna, AT
SEBASTIAN SCHWAMBERGER, University of Vienna, Vienna, AT

ALI MEMBERS CONSULTATIVE GROUP

Principles for a Data Economy
(as of April 29, 2021)

MARC T. AMY, Lafayette, LA
CHRISTOPHER EDWARD APPEL, Washington, DC
TOM BAKER, Philadelphia, PA
IAN C. BALLON, East Palo Alto, CA
JOSEPH R. BANKOFF, Atlanta, GA
PETER V. BAUGHER, Chicago, IL
SHAWN J. BAYERN, Tallahassee, FL
MICHAEL M. BAYLSON, Philadelphia, PA
SPYRIDON V. BAZINAS, Vienna, Austria
JEFFREY A. BEAVER, Seattle, WA
MARY BECKMAN, Boston, MA
ASHUTOSH A. BHAGWAT, Davis, CA
MATTHEW T. BODIE, Saint Louis, MO
WILLARD L. BOYD III, Des Moines, IA
HARVEY G. BROWN JR., Houston, TX
TIMOTHY W. BURNS, Madison, WI
JOHN P. BURTON, Santa Fe, NM
STEPHEN CALKINS, Detroit, MI
JONATHAN G. CEDARBAUM, Washington, DC
COLLEEN V. CHIEN, Santa Clara, CA
SYLVIA FUNG CHIN, New York, NY
YEE WAH CHIN, New York, NY
WAYNE DALE COLLINS, Washington, DC
GIOVANNI COMANDÉ, Pisa, Italy
MICHELLE WILLIAMS COURT, Los Angeles, CA
ANUJ C. DESAI, Madison, WI
ROBERT P. DEYLING, Washington, DC
TOBIAS A. DORSEY, Silver Spring, MD
CHRISTOPHER R. DRAHOZAL, Lawrence, KS
MAREK DUBOVEC, Tucson, AZ
ARTHUR W. S. DUFF, Greenbrae, CA
RICHARD L. FIELD, Cliffside Park, NJ
DANIEL M. FILLER, Philadelphia, PA
MARK E. FOSTER, Ann Arbor, MI
MEREDITH FUCHS, Washington, DC
HENRY D. GABRIEL, Greensboro, NC
MARVIN GARFINKEL, Gladwyne, PA
LLEWELLYN JOSEPH GIBBONS, Toledo, OH
DANIEL C. GIRARD, San Francisco, CA
DOROTHY J. GLANCY, Santa Clara, CA
PHILIP S. GOLDBERG, Washington, DC
JOHN M. GOLDEN, Austin, TX
DAVID C. GRAY, Baltimore, MD
I. MICHAEL GREENBERGER, Baltimore, MD
CHARLES E. GRIFFIN, Ridgeland, MS
DAVID W. GRUNING, Abita Springs, LA
PETER E. HALLE, Coconut Grove, FL
RICHARD ANTHONY HODYL JR., Chicago, IL
EDWIN E. HUDDLESON, Washington, DC
HOWARD O. HUNTER, Singapore, Singapore
ROBERT A. JAMES, San Francisco, CA
KIRK C. JENKINS, Half Moon Bay, CA
SANDRA A. JESKIE, San Diego, CA
DALIÉ JIMÉNEZ, Irvine, CA
KRISTIN N. JOHNSON, Atlanta, GA
CURTIS E.A. KARNOW, San Francisco, CA
AMY KELLER, Chicago, IL
CATHERINE KESSEDJIAN, Paris, France
NANCY S. KIM, San Diego, CA
CHRISTOPHER M. KLEIN, Vancouver, WA
RENEE KNAKE JEFFERSON, Houston, TX
PETER R. KOCHENBURGER, Hartford, CT
DAVID N. KRAGSETH, Philadelphia, PA
WILLIAM K. KROGER, Houston, TX
JOHN LINARELLI, Central Islip, NY
HOUSTON PUTNAM LOWRY, Hartford, CT
THOMAS S. LUE, Mountain View, CA
MEGHAN H. MAGRUDER, Atlanta, GA
C. SCOTT MARAVILLA, Washington, DC
LORELIE S. MASTERS, Washington, DC
JAMES C. MCKAY JR., Washington, DC
A. DOUGLAS MELAMED, Stanford, CA
CHARLES W. MOONEY JR., Philadelphia, PA
JULIET M. MORINGIELLO, Harrisburg, PA
BARAK ORBACH, Tucson, AZ
NANCY LEEDS PERKINS, Washington, DC
JEFFREY M. POLLOCK, Princeton, NJ
IAIN D. C. RAMSAY, Canterbury, England
R. ANTHONY REESE, Irvine, CA
DAN ROBBINS, Calabasas, CA
JACOB H. ROOKSBY, Spokane, WA
KEITH A. ROWLEY, Las Vegas, NV
HANS SCHULTE-NÖLKE, Osnabruck, Germany
VICTOR E. SCHWARTZ, Washington, DC
PAUL M. SECUNDA, Milwaukee, WI
JOAQUIN SILGUERO ESTAGNAN, Belgique, Spain
KENNETH W. SIMONS, Irvine, CA
DAVID L. SLOSS, Santa Clara, CA
GEORGE PRESCOTT SLOVER, Washington, DC
DOUGLAS G. SMITH, Chicago, IL

MARY L. SMITH, Lansing, IL
LYNN A. SOUKUP, Washington, DC
PAUL B. STEPHAN, Charlottesville, VA
H. MARK STICHEL, Baltimore, MD
GUY MILLER STRUVE, New York, NY
MARY-CHRISTINE SUNGAILA, Irvine, CA
RICK SWEDLOFF, Camden, NJ
LOUISE ELLEN TEITZ, Bristol, RI
LUCY L. THOMSON, Washington, DC
MICHAEL A. TRONCOSO, Atlanta, GA
SJEF VAN ERP, Maastricht, Netherlands
ARI EZRA WALDMAN, Boston, MA
LAUREN E. WILLIS, Los Angeles, CA
JANE K. WINN, Seattle, WA
PETER A. WINN, Washington, DC
CHRISTOPHER WOLF, Washington, DC
PETER K. YU, Fort Worth, TX

ELI MEMBERS CONSULTATIVE COMMITTEE

Principles for a Data Economy
(as of April 7, 2021)

NAHEL ASFOUR, Tel-Aviv University, ISR

FRANCESCO AVOLIO, Bar Council of Naples, IT

MARIANGELA BALESTRA, Lex IBC, IT

ELENA BARGELLI, University of Pisa, IT

DANIEL BERLINGER REMUS, Faculty of Law of the Western University "Vasile Goldis" of Arad, RO

WOJCIECH BIERNACKI, Adam Mickiewicz University in Poznań, PL

MARCO BOTTA, Max Planck Institute for Innovation and Competition, IT

TIMOTHY BURNS, American Constitution Society, USA

CHRISTOPH BUSCH, University of Osnabrück, DE

MICHEL CANNARSA, University of Lyon, FR

LUCA CASTELLANI, UNCITRAL, IT

ANA MARÍA CEDIEL SERRA, Lawyer, ES

ROSELLA ESTHER CERCHIA, Società Italiana per la Ricerca nel Diritto Comparato, IT

ROSSANA DUCATO, UCLouvain and Université Saint-Louis, Bruxelles, IT

MATEJA DUROVIC, Dickson Poon School of Law, RS

WIAN ERLANK, Law Faculty, North-West University, Potchefstroom Campus, RPA

HANO ERNST, Faculty of Law of the University of Zagreb, HR

FABIO FERRARO, University of Naples, IT

CAROLINE FREDRICKSON, American Constitution Society, USA

JOSE CARAMELO GOMES, Portucalense Institute for Legal Research, PT

SZILVIA ZSUZSANNA GÖLLEY, Curia of Hungary, HU

MATEUSZ GROCHOWSKI, Institute of Legal Studies, Polish Academy of Sciences, PL

HANA HORAK, Zagreb University, HR

INA HOXHAJ, Supreme Court of Albania, AL

KANITA IMAMOVIC-CIZMIC, Faculty of Law of the University of Sarajevo, BA

TATJANA JOSIPOVIĆ, Zagreb University, HR

MAGDALENA KĘDZIOR, Academy of European Law, PL

ZSUZSANA KOVÁCS, Curia of Hungary, HU

ALEXANDER KUNZELMANN, UNCITRAL, AU

GABRIEL ALONSO LANDETA, Colegio de Registradores de la Propiedad y Mercantiles de España, ES

DACE LUTERS-THÜMMEL, European Women Lawyers Association (EWLA), LV

ATTILA MENYHÁRD, Faculty of Law of the Eötvös Loránd University, HU

HENDRIK MILDEBRATH, Europa-Universität Viadrina, DE

KATHARINA MILLER, European Women Lawyers Association (EWLA), ES

ANCA MOROȘTEȘ, Faculty of Law of the Western University "Vasile Goldis" of Arad, RO

MELIHA POVLAKIC, University of Sarajevo, BA

GONZALO VILLALTA PUIG, School of Law of the University of Hull, ES

ANDREA PURPURA, Kore University of Enna, IT

ALBERT RUDA, University of Girona, ES

LEIGH SAGAR, Society of Trust and Estate Practitioners (STEP), UK

MARTA SANTOS SILVA, University of Maastricht, Faculty of Law, Private Law Department, PT

MATTHIAS SCHMIDL, Austrian Data Protection Authority, AT

HANS SCHULTE-NÖLKE, University of Osnabrück, DE

RAINER SEDELMAYER, European Union of Judges in Commercial Matters, AT

ROB VAN DE WESTERLAKEN, European Parliament, NL

REPORTERS' PREFACE

Discussions about a joint project between The American Law Institute (ALI) and the European Law Institute (ELI) in the field of the data economy started in 2016. Meetings with a view to conducting a mapping exercise included workshops in October 2016 in New York, New York, and in March 2017 in Vienna, Austria. A Draft Framework for Discussion dated 25 August 2017 by CHRISTIANE WENDEHORST, NEIL COHEN, and STEVE WEISE was presented at the ELI Annual Conference in Vienna on 7 September 2017. This document was intended to demonstrate that it is both feasible and timely to formulate ALI-ELI Principles for a Data Economy, presenting a first tentative draft of what such Principles could look like. The project was adopted by the ALI Council on 19 January 2018 and by the ELI Council on 9 February 2018, appointing NEIL COHEN and CHRISTIANE WENDEHORST as Reporters, and STEVE WEISE and THE LORD JOHN THOMAS OF CWMGIEDD as Chairs coordinating a wider group of advisers from both the ALI and the ELI.

Members of this group convened in New York on 15 and 16 February 2018 to advise the Reporters concerning the overall direction of the project. The Reporters produced a Pre-Draft dated 20 August 2018 that was presented at the ELI Annual Conference in Riga, Latvia, on 6 September and discussed in detail with ELI Advisors and the ELI Members Consultative Committee (MCC) on 8 September 2018. Considering guidance received at this meeting, the document was submitted as Preliminary Draft No. 1 to the ALI Advisers and Members Consultative Group (MCG) in Philadelphia, Pennsylvania, on 25 and 26 October 2018. Both meetings together resulted in a broad range of changes, including a reordering of the Parts and a clearer focus on the transactional aspects, reflected in Preliminary Draft No. 2, dated 4 February 2019, and discussed at a joint meeting with the ALI and ELI Advisers/Advisors and MCG/MCC in Philadelphia on 22 February 2019. An interim Preliminary Draft No. 2*bis* was discussed with ELI Advisors and MCC in Vienna on 3 September 2019, resulting in Preliminary Draft No. 3, which was completed on 15 October and discussed with ALI Advisers and MCG in Philadelphia on 31 October 2019. It took on board guidance received since the earlier 2019 meetings, including scrutiny undertaken by the Berlin-based tech company acs-plus GmbH, suggestions from the industry, and inspirations gained at a meeting hosted jointly by the United Nations Commission on International Trade Law (UNCITRAL) and French governmental institutions in Paris, France, on 15 March 2019 as well as at the 52nd Commission session of UNCITRAL in

Vienna on 17 July 2019. It also took on board inspiration gained from other international sources such as the Contract Guidelines on Utilization of AI and Data (Data Section) from June 2018, issued by the Japanese Ministry of Economy, Trade and Industry (referred to as "METI Guidelines") as well as the first report on collected model contract terms of the Support Centre for Data Sharing which was initiated by the European Commission in early 2019.

On the basis of guidance received at and after the 31 October 2019 meeting, Principles 1 to 10 and 16 to 23 (then 15 to 22) were submitted as ALI Council Draft No. 1 to the ALI Council for its meeting on 17 January 2020 and approved that day. Taking on board further guidance received by ALI and ELI members, UNCITRAL Working Group No. IV on Electronic Commerce on 28 November 2019, the participants of a conference hosted by the German Ministry of Justice on 12 and 13 December 2019 in Berlin, Germany, the ELI Council on 20 and 21 February 2020, and the participants of an expert workshop hosted by UNCITRAL and the International Institute for the Unification of Private Law (UNIDROIT) on 10 and 11 March 2020 in Vienna, the Reporters produced Tentative Draft No. 1. The latter was submitted electronically for consultation to the members of the ALI, in lieu of submission for approval at the 2020 Annual Meeting (canceled due to the COVID-19 situation). Tentative Draft No. 1 was further submitted to the members of the ELI Advisors and MCC for their remote meeting on 22 June 2020. The guidance received led to the production of Preliminary Draft No. 4, which was presented to the ELI Members at the ELI Annual Conference on 10 September 2020 and later discussed with ALI and ELI Advisers/Advisors and MCG/MCC at a remote meeting on 8 October 2020. With the feedback received, including the feedback received at an international conference cohosted by UNCITRAL and the Japanese government on 10 September 2020, from members of the Data Governance Working Group of the Global Partnership on AI (GPAI), as well as from the Federation of German Industries at a meeting on 4 December 2020, the Reporters produced Council Draft No. 2, which was submitted to the ALI Council for its meeting on 21 January 2021 and approved that day.

Taking on board guidance received during the ALI Council meeting, a joint meeting with the ALI and ELI Advisers/Advisors and MCG/MCC on 8 February 2021, and the meeting of the ELI Council on 11 February 2021, the Reporters produced Tentative Draft No. 2, which was submitted to the ALI membership for its remote 2021 Annual Meeting on 18 May 2021. After the approval by the ALI membership and a joint meeting held with the ALI and ELI

Advisers/Advisors and MCG/MCC on 28 June 2021, the Reporters produced the ELI Final Council Draft, which was submitted to the ELI Council for their meeting on 1 September 2021 and approved that day. Finally, the draft was also approved by the ELI Membership on 24 September 2021.

The approved ALI-ELI Principles for a Data Economy have been presented to the broad public and been discussed with experts from various institutions around the world at the Principles for a Data Economy Conference on 18 and 19 October 2021. After making some minor adjustments, taking into account guidance received, in particular, by the bodies of the ALI and ELI, the Reporters updated the Reporters' Notes to reflect the legal situation as of 28 February 2022 and produced this final version of the ALI-ELI Principles for a Data Economy.

On the European side, the project is generously funded by the Fritz Thyssen Foundation

TABLE OF CONTENTS

Section *Page*

Introductory Note 1

PART I
GENERAL PROVISIONS

Principle 1. Purpose of these Principles 8
Principle 2. Scope of these Principles 16
Principle 3. Definitions 21
Principle 4. Remedies 37

PART II
DATA CONTRACTS

CHAPTER A
RULES AND PRINCIPLES GOVERNING DATA CONTRACTS

Principle 5. Application of these Principles to Data Contracts 42
Principle 6. Interpretation and Application of Contract Law 48

CHAPTER B
CONTRACTS FOR SUPPLY OR SHARING OF DATA

Principle 7. Contracts for the Transfer of Data 52
Principle 8. Contracts for Simple Access to Data 67
Principle 9. Contracts for Exploitation of a Data Source 74
Principle 10. Contracts for Authorization to Access Data 79
Principle 11. Contracts for Data Pooling 84

CHAPTER C
CONTRACTS FOR SERVICES WITH REGARD TO DATA

Principle 12. Contracts for the Processing of Data 91
Principle 13. Data Trust Contracts 99
Principle 14. Data Escrow Contracts 110
Principle 15. Data Marketplace Contracts 116

PART III
DATA RIGHTS

CHAPTER A
RULES AND PRINCIPLES GOVERNING DATA RIGHTS

Principle 16. Data Rights 122
Principle 17. Application of these Principles to Data Rights 128

CHAPTER B
DATA RIGHTS WITH REGARD TO CO-GENERATED DATA

Principle 18. Co-Generated Data 132
Principle 19. General Factors Determining Rights in Co-Generated Data 140
Principle 20. Access or Porting with regard to Co-Generated Data 147
Principle 21. Desistance from Data Activities with regard to Co-Generated Data 158
Principle 22. Correction of Co-Generated Data 163
Principle 23. Economic Share in Profits Derived from Co-Generated Data 165

CHAPTER C
DATA RIGHTS FOR THE PUBLIC INTEREST

Principle 24. Justification for Data Rights and Obligations 170

Principle 25. Granting of Data Access by the Controller 178
Principle 26. Data Activities by Recipient..... 182
Principle 27. Reciprocity 188

PART IV
THIRD PARTY ASPECTS OF DATA ACTIVITIES

CHAPTER A
PROTECTION OF OTHERS AGAINST DATA ACTIVITIES

Principle 28. Wrongfulness of Data Activities vis-à-vis Another Party..... 191
Principle 29. Rights that Have Third-Party Effect Per Se 197
Principle 30. Contractual Limitations..... 204
Principle 31. Unauthorized Access..... 210

CHAPTER B
EFFECTS OF ONWARD SUPPLY ON THE PROTECTION OF OTHERS

Principle 32. Duties of a Supplier in the Context of Onward Supply..... 214
Principle 33. Direct Action against Downstream Recipient..... 222
Principle 34. Wrongfulness Taking Effect vis-à-vis Downstream Recipient..... 226

CHAPTER C
EFFECTS OF OTHER DATA ACTIVITIES ON THE PROTECTION OF THIRD PARTIES

Principle 35. Duties of a Controller with regard to Data Processing and Derived Data..... 236
Principle 36. Wrongful Processing..... 243
Principle 37. Effect of Nonmaterial Noncompliance..... 249

PART V
MULTI-STATE ISSUES

Principle 38. Application of Established Choice-of-Law Rules of the Forum 253
Principle 39. Issues Not Covered by Established Choice-of-Law Rules of the Forum 261
Principle 40. Relevance of Storage Location 264

Cite thus:

Principles for a Data Economy: Data Transactions and Data Rights, Principle ___

INTRODUCTORY NOTE

The law governing trades in commerce in the United States and in Europe has historically focused on trade in items that are either real property, goods, or intangible assets such as shares, receivables, intellectual property rights, licenses, etc. With the emergence of the data economy, however, tradeable items often cannot readily be classified as such goods or rights, and they are arguably not services. They are often simply "data." Both in the United States and in Europe, uncertainty as to the applicable rules and doctrines to govern the data economy is beginning to trouble stakeholders (such as data-driven industries, micro, small and medium-sized enterprises, as well as consumers). This uncertainty undermines the predictability necessary for efficient transactions in data, may inhibit innovation and growth, and may lead to market failure and manifest unfairness, in particular for the weaker party in a commercial relationship.

A. Why Principles on Data Transactions and Data Rights?

The application of traditional legal doctrines to trades in data is not well developed, often does not fit the trade, and is not always useful or appropriate or even accomplished in a consistent manner. At the bottom of this uncertainty lies the fact that data is different from other resources in several ways, such as by being what has come to be called a "non-rivalrous resource," i.e., data can be multiplied at basically no cost and can be used in parallel for a variety of different purposes by many different people at the same time. When A sells a machine to B, A will no longer have the machine, but when A sells data to B, both A and B can have and use the data, and the multiplication of the data does not in any way reduce its practical utility (without prejudice to the fact that the market value of data may decrease rapidly with increasing numbers of persons having the data). Also, the way data can be shared or supplied differs significantly from the way goods are made available to others, and many transactions in the data economy do not have an analogy in traditional commerce. If A allows B to access data in a secure space on A's servers with an algorithm to run certain processing activities, this would be a very common type of transaction in the data economy, but there is no established body of applicable contract law that would fit precisely this type of transaction.

However, data is also different from intellectual property as, in the transactions usually considered to be part of the "data economy," what is "sold" is not the permission to utilize an intangible but rather binary impulses with a particular meaning, usually as "bulk" or "serial" data. This focus on binary impulses in large batches, which may be stored, transmitted, processed with

the help of machines, etc., is also what differentiates transactions in the data economy from traditional information services. When A pays B for gathering information on election outcomes in a foreign country, the focus is on B *doing* something (i.e., telling A, even if A and B have agreed B must give A the information in a particular format, such as by email). By contrast, when A pays B for real time transmission of exit-poll data to be displayed on A's news channel, the focus is on B *delivering* something (i.e., a large batch of binary impulses with a particular meaning in a particular format).

The fact that data is different is the reason why it has become necessary to draft principles for data transactions and data rights instead of merely referring to the existing law of, say, sale and lease of goods, or of services. It is important to note that the legal analysis depends to a great degree on whether the relevant data is protected under rules such as intellectual property law or trade secret law and/or rules that limit certain types of conduct (such as data privacy/data protection law and consumer protection law).

This project seeks to propose a set of principles that might be implemented in any kind of legal environment, and to work in conjunction with any kind of data privacy/data protection law, intellectual property law, or trade secret law, without addressing or seeking to change any of the substantive rules of these bodies of law.

B. Players and Relations in the Data Ecosystem

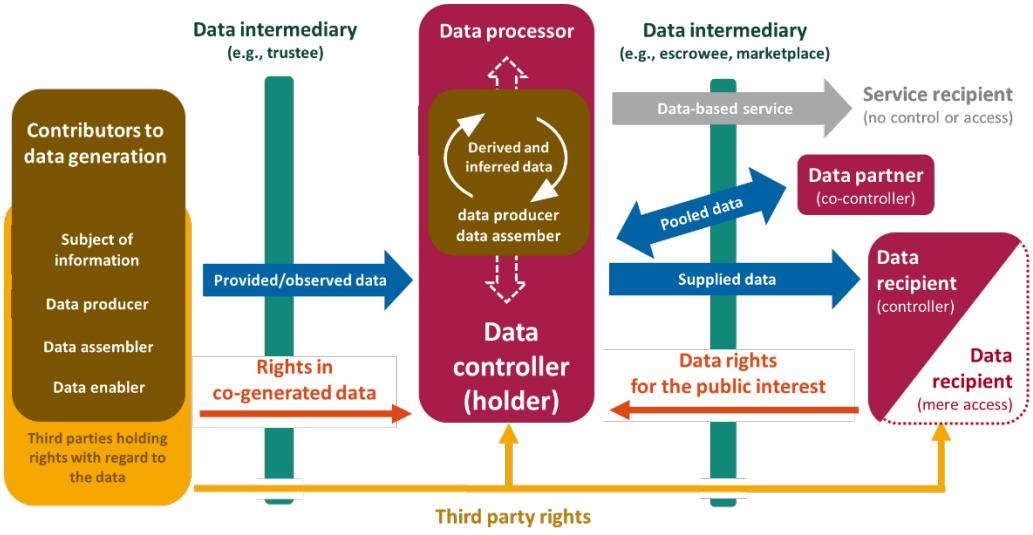
These Principles cannot provide a complete set of standards for any sort of dealings within the data economy. This is so for a variety of reasons, including the special dynamics of the data economy as a fast-moving field, the desire to reduce complexity and focus these Principles on some central points, and the need to produce something that works in vastly differing legal environments in different regions of the world.

These Principles have taken the basic types of players and relations that we find in data ecosystems as a starting point. The central player in all data ecosystems is the controller (often also called the "holder") of data, i.e., the party that is in a position to access the data and that decides about the purposes and means of their processing. That controller may exercise control all by itself or share it with co-controllers, such as under a data pooling arrangement. A (mere) processor of data, on the other hand, is a service provider that processes data on a controller's behalf.

There is also a variety of different parties contributing in different ways to the generation of data. One important way of contributing to the generation of data is by being the individual or legal entity that is the subject of the information recorded in the data. Another way of contributing to the generation of data is by being a data producer, i.e., generating data in the sense of recording information that had previously not been recorded. There are also parties that do not produce data in this sense, but create added value by assembling data in some meaningful ways, and parties that contribute in more remote roles. The parties that contribute to the generation of data may provide the data to the controller (provided data). Data may be produced by the controller itself through observing the parties (observed data). The controller may also obtain derived or inferred data from data that has been observed or provided.

A controller of data often supplies the data to third-party data recipients, in particular under contractual or other data sharing arrangements. Recipients of data may become new controllers when data is fully transferred to them, or they may receive only access to the data, such as when they are permitted to process data with a mobile software agent on the supplier's server. Needless to say, an important part of the data economy consists in using data for creating new value, such as by developing and marketing data-based products and services; marketing these products and services is, however, not covered by these Principles.

In addition to the parties mentioned, there are an increasing number of different types of data intermediaries, such as data trustees, data escrowees, or data marketplace providers. They facilitate the transactions between the different actors, in particular between parties generating data and data controllers, and between data suppliers and data recipients, such as by acting as a trusted third party. The following figure visualizes in a simplified manner how these players interact with each other.



C. Structure of these Principles

a. Part I. General Provisions. The first Part sets out the purpose and scope of these Principles and provides definitions of key terms that they utilize, such as "data," "copy," "processing," "control of data," and "supply" of data. In defining these terms, efforts have been made to ensure consistency with both established terminology worldwide and other ALI and ELI work. Finally, Part I addresses these Principles' impact on remedies.

b. Part II. Data Contracts. The second Part of these Principles is devoted to contracts the subject of which is data, establishing, in the first place, sets of default terms appropriate for different basic types of data transactions. While focusing on contracts, the default terms apply also, with appropriate adjustments, to the governing principles of similar arrangements, such as when a company or other legal entity is established instead (e.g., for a data pooling arrangement). Part II begins by setting out, in Chapter A, some general provisions on the interpretation and application of these Principles to data contracts, including a general hierarchy for determining the rules governing data contracts.

Chapter B is more specifically about contracts for supply or sharing of data. These Principles identify, as a first step, typical contractual promises in the data economy that involve different types and modalities of provision of data, and show how these transactions in the data economy can be systematized, with a view to analyzing the rights and obligations of the parties to the transaction. These rights and obligations may be very different, depending on whether, e.g., a party has promised to fully transfer data to a medium within the recipient's sphere of control, or only to grant access to a medium on which data is stored or maybe even only to consent to the collecting and processing of data by the other party to the transaction while refusing to take any responsibility for what the other party ultimately receives. When data is not just provided by a supplier to a recipient, but two or several parties decide to contribute data to a data pool or closed platform each of them has access to, this again may require a somewhat different set of rules. It should be noted that the terms "supply" and "sharing" may, by and large, be used interchangeably, even though "supply" fits better to describe a one-way provision of data. Among the policy choices recommended by these Principles in the context of supply or sharing of data is the default position that, when the data is fully transferred, the data may be used by the recipient for any lawful purpose that does not infringe the rights of third parties. (Thus, these Principles take a "sales approach" as opposed to a "license approach.") Because, however, these Principles provide a wide berth for private ordering, including provisions that emphasize freedom of contract except when limited by

a mandatory rule of the applicable jurisdiction, parties will remain able to agree on arrangements close to a "data license," as is frequently found in model agreements and in data contracts (even when the data is not protected by intellectual property law). For contracts in which the recipient is given only simple access to data on a medium controlled by the supplier, these Principles suggest the opposite default position (i.e., a "license approach").

Chapter C deals with contracts whose focus is not the provision of data by one party to another, or the sharing of data among various parties, but rather the provision of services with regard to data. The most important contract type in this regard is contracts for the processing of data, including any cloud storage of data and any data analytics. Another type of contract addressed in Chapter C is a type that has been labeled, for lack of a better term, "data trust contracts," although that term should not be taken as encompassing the specific legal implications of the common-law concept of trusts, and a related type of contract labeled "data escrow contracts." Also, data marketplace contracts, which are essentially about the facilitation of data transactions and the matchmaking between parties, are dealt with under this Part.

c. Part III. Data Rights. The third Part of these Principles is devoted to data rights. It is important to note that Part III goes beyond the type of relationships addressed in Part II. Much of the data economy is not about "pure data commerce," such as a data broker selling data to an advertising agency, but about very traditional value chains, involving, e.g., suppliers of components, producers, wholesalers, retailers, and end users, with data being generated at various links in that chain. When parties in that value chain make arrangements about data, e.g., the producer allows the supplier of a component to access data relating to the performance of that component in the producer's cloud, this is then a contract within the meaning of Part II (e.g., a contract for simple access to data under Principle 8). In practice, however, parties have often not made proper arrangements concerning such data, which is why Principles are required for outlining to what extent notions of fundamental fairness dictate that such arrangements be made. Typical data rights are access and porting rights, as well as rights to request desistance from a particular data use, correction of data, or even a share in proceeds from data activities. Like the previous Part, Part III starts with a Chapter A on general rules and principles governing data rights.

Part III, Chapter B, identifies, analyzes, and collates existing and potential future rules on data rights with regard to what these Principles call "co-generated data." The fact that a party had a share in the generation of certain data—such as by being the subject of the information coded in the data, or owning the device by which data has been generated, or having designed the device

with the help of which data is generated—may, together with other factors, give rise to a special relationship between that party and any controller of the data. For example, an important part of the data economy is the supply of goods, digital content (such as software), and services to customers when, through the use of these commodities by the customers or other users, data is generated and transmitted to and ultimately processed by the supplier or producer of the commodity or any other third party chosen by the supplier or the producer. These Principles analyze, inter alia, the situation of customers with regard to user-generated data, addressing intricate legal issues such as a customer's access and porting rights, e.g., when the customer wishes to resell the commodity or to switch the supplier of a digital service, as well as other typical constellations in data value chains.

While these Principles do not intend to engage in the scholarly debate between "privacy theories" and "property theories," it ought to be noted that the "co-generated data" approach, which has been developed by these Principles and is gaining recognition worldwide, transcends the debate. It does so by combining elements of both theories in a scheme of fairness rules that has been developed specifically with a view to the characteristics of data as a non-rivalrous, multi-functional, and extremely dynamic resource.

Chapter C on other data rights addresses data rights that are afforded to a party without regard to any share the party may have had in the generation of the data. Such rights are typically afforded for public interest purposes, including for the purpose of ensuring fair and undistorted competition and the purpose of making data openly available in order to foster general innovation and growth. Given the broad variety of these data rights, Chapter C states only some very general principles, such as those concerning proportionality, access under FRAND (fair, reasonable, and nondiscriminatory) conditions, protection of third-party rights, a no-harm principle, and reciprocity.

d. Part IV. Third-Party Aspects of Data Activities. Part IV deals with third-party aspects of the data activities addressed under the preceding Parts of these Principles. While, e.g., supply or sharing of data are, primarily, about a transaction between two or more parties and about the contractual rights and remedies those parties may have against each other, there are also third parties who may be affected by the transaction and who may have a word to say. This may be the case, e.g., when the onward transfer of data interferes with a right of another party, such as an intellectual property right or a right flowing from data privacy/data protection law.

Chapter A sets out general considerations about when data activities are wrongful vis-à-vis protected parties, including situations in which data activities fail to comply with contractual limitations, or in which access to data has been obtained by unauthorized means.

Onward supply of data by a controller may affect such protected parties. Among other things, clarity must be achieved as to whether and to what extent contractual protection against certain downstream data activities is possible, and what the effect would be on downstream recipients. These Principles suggest, in Part IV, Chapter B, that contractual limitations on data activities may have downstream, third-party effects under a tort-like regime inspired by trade secrets law, and the same would apply when data had originally been obtained by unauthorized means before being passed on. In suggesting this regime, these Principles seek to strike a balance between the desire to ensure strong protection of existing rights on the one hand and the desire to encourage data sharing and create an economy-friendly environment on the other. Chapter B also deals with the general due diligence duties of parties that pass data on to downstream recipients, and with possibilities to take direct action against downstream recipients.

Part IV, Chapter C, addresses the situation in which data has been aggregated with other data, or has otherwise been processed so as to obtain derived data. Clarity must be achieved as to whether limitations following from third-party rights with regard to the original data set still apply with regard to the derived data set, what the legal consequences are if the answer is yes, and whether any legal consequences with regard to the derived data set follow from the mere fact that the data set has been derived by way of wrongful processing activities.

e. Part V. Multi-State Issues. Transactions and other activities in the data economy will, by their very nature, hardly ever occur within the confines of national borders. Accordingly, the last Part, without purporting to provide a complete set of choice-of-law or similar rules, provides some guidance as to the application of rules and doctrines of private international law to issues in the data economy.

PART I
GENERAL PROVISIONS

Principle 1. Purpose of these Principles

(1) These Principles are intended for use in legal systems in Europe, the United States, and elsewhere. They are designed to:

(a) bring coherence to, and move toward harmonization of, existing law and legal concepts relevant for the data economy;

(b) be used as a source to inspire and guide the further development of the law by courts and legislators worldwide;

(c) inform the development of best practices and guide the development of emerging standards, including standards or trade codes that are specific to a particular industry or industry sector;

(d) facilitate the drafting of model agreements or provisions to be used on a voluntary basis by parties in the data economy;

(e) govern contracts or complement the law that governs them to the extent that they provide default rules or that parties to a transaction have incorporated them into their contract or have otherwise designated them to govern; and

(f) guide the deliberations of tribunals in arbitration and other dispute resolution forums.

(2) These Principles recommend a legal framework that is intended to work with any form of data privacy or data protection law, intellectual property law, or trade secrets law. These Principles are not intended to amend or create any such law, but they may inform the development of such law. In the event of any inconsistency between these Principles and such other law that cannot be overcome by interpretation, the other law should prevail.

Comment:

a. Addressees and added value. These Principles address a fast-emerging but already major sector of the economy. Yet, this sector has developed largely without a legal framework that recognizes and reflects many of the sector's important and unique attributes in order to govern it in a way that thoughtfully balances and facilitates both the public interest and the private interests of the parties. These Principles are the result of collaborative work of lawyers from Europe and

the United States. They are designed to provide guidance as to the basic principles to be applied to data transactions and related matters irrespective of the otherwise applicable legal framework (whether that of a U.S. state or one of the European legal systems), and thereby seek to develop a consistent, general approach across national borders and legal disciplines.

The purpose of these Principles is to provide guidance to and to inform parties, practitioners, arbitral tribunals, standardization bodies, courts, and legislators worldwide. They seek to promote the enhancement and better adaptation of the law to the data economy as an ever more important part of the economy at large, and to identify guiding principles in dealing with data as an asset and tradeable item. By doing so, they facilitate the further development of the law by courts and legislators worldwide, and the review of existing law and soft law instruments by, in particular, legislative bodies, standardization agencies, or bodies developing codes of conduct. These Principles are also designed to facilitate the drafting of model agreements or provisions to be used on a voluntary basis by parties in the data economy. Equally, they may govern contracts or complement the law that governs contracts to the extent that they provide default rules or that parties to a transaction have incorporated them into their contract or have otherwise designated them to govern. These Principles may, in a similar vein, guide the deliberations of tribunals in arbitration and other dispute resolution forums (such as mediation). Depending on the specific needs and characteristics of a particular industry, these Principles may provide the basis for adaptation or extension for the development of industry-specific standards.

By their very nature, some Parts of these Principles are addressed to particular players more than to others. For instance, Part II on data contracts is addressed both to parties in the data economy (and to counsel advising those parties), bringing some clarity as to the main types of transactions and suggesting rules that could typically be considered reasonable and fair, and to courts, which must deal with incomplete agreements and provide appropriate "gap fillers" when parties have failed to deal with important issues. Part III on Data Rights is predominantly addressed to legislators and bodies developing standards and codes of conduct. However, it is also addressed to parties, their legal advisers, and to courts dealing with issues that involve the relationship between, e.g., the users of goods, digital content, or services and the manufacturer, or between the manufacturer and suppliers of components. Part IV may be seen to be addressed primarily to legislators considering issues raised by the data economy, and to courts that have been called upon by a party, e.g., because that party claims its rights have been infringed by some data activity. The same would hold true for Part V dealing with cross-border issues. However, none of the Parts is

exclusively targeted at the specific audiences just mentioned, and these Principles seek to provide added value to as broad a variety of actors as possible.

b. Relationship with specific areas of the law not addressed by these Principles. The data economy is a subject that touches upon and cuts across many areas of the law. Most notably, data may in many instances be protected by copyright or other intellectual property rights. In addition, to the extent that data is personal data (i.e., data relating to an identified, or identifiable, natural person), data privacy/data protection law provides for an ever more comprehensive set of rules. Another area of the law with a firmly established framework that addresses the protection of information and data is trade secret law. While these Principles cannot entirely avoid referring to these areas of the law, they do not seek to restate what the rules in those areas are or should be. Rather, they take those areas of the law as more or less given.

For example, these Principles propose rules to govern transactions in nonpersonal data as well as personal data, recognizing that the latter type of data may be subject to data privacy/data protection regimes. These Principles, in some cases, address some implications of such regimes for trade in data. But these Principles do not deal with issues fully covered by data privacy/data protection law, such as when consent is necessary and/or can be withdrawn.

Illustration:

1. Business S supplies an online video game and holds a broad range of personal data from users playing that game, much of which is protected under data privacy regimes such as the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR). S "sells" the data of 20,000 users to data analytics business R in a way that is in conformity with the relevant data privacy regimes. Shortly after the data is transferred to R, 5,000 users from the European Union withdraw their consent to the processing of the data. As a reaction, R demands return of 25 percent of the price paid to S. As these Principles do not seek to restate or revise data privacy/data protection law, they do not deal with questions such as whether the users' consent may be withdrawn at any time, or whether the users have a right to object to the sale by clicking a button stating "Do not sell my data" or the like. Rather, user rights under data privacy/data protection law are left to the applicable rules, considering also the territorial scope of those rules. These Principles do, however, address the effect of data privacy/data protection regimes, and of rights exercised under such regimes, on the rights of parties to a data transaction such as

the transaction between S and B, e.g., whether S would have been under a duty to make R aware of this risk and whether R has any rights against S because R ultimately lost 25 percent of what R had bargained for.

Sometimes, the validity of a transaction dealt with under these Principles will depend on such other law, e.g., when a transaction is blatantly inconsistent with data privacy/data protection law that may, depending on the circumstances, mean the transaction is illegal and thus void or voidable under the applicable law. That, too, is not a matter for these Principles to deal with.

Illustration:

2. Assuming that, in a scenario such as that in Illustration no. 1, a large number of users failed to give their consent, or clicked the button "Do not sell my data," and thus "sale" and transfer of the data by S to R was in violation of an applicable data protection regime, and both S and R were aware of that. Whether that affects in any way the validity of the contract between S and R is not dealt with in these Principles. However, these Principles do deal with what the unwinding of the transaction means with regard to the data.

Sometimes, different aspects of the same activity may be the subject of these Principles as well as other bodies of law. For instance, data porting (portability) rights are dealt with under Part III of these Principles, but they may also be an element of data protection law, consumer protection law, or competition law. It is, in particular, in those grey zones that the other bodies of law would prevail in the event of any inescapable inconsistency between them and these Principles, but still these Principles might inform the development of those other bodies of law and point at directions of development that might be more favorable than others for a flourishing data economy. For example, a major challenge for the data economy is that there is hardly any data pool that does not implicate potential issues arising from data privacy/protection law (e.g., because some data in the pool is personal data, or can be de-anonymized in the future), intellectual property law (e.g., because some snippets of text might be protected by copyright), or trade secrets law (e.g., because aggregated machine data allow conclusions about business operations). This leads to reluctance on the part of businesses to share their data with others, as such sharing might indirectly expose them to requests for erasure, claims for damages, and other adverse consequences. The law should take

these considerations into account when accommodating these diverse needs, and Principles 34, 36, and 37 in particular make some suggestions as to how this could be achieved.

c. Relationship with contract rules and doctrines. The relationship of these Principles to existing law of sales and service contracts, such as can be found in European civil codes or in the Uniform Commercial Code or other statutes, is an entirely different story. There is a clear overlap between such areas of the law and these Principles, such as with regard to contractual rights and obligations of the parties. These Principles are inspired by those bodies of law and are guided by them, sometimes clarifying application of existing principles in the data context while other times providing a roadmap for future development. They seek to identify standards that, if adopted, would take priority over existing rules in these areas by tailoring their application to data transactions. The same holds true for unfair competition law, which, however, normally does not specifically deal with data or information and would be informed by these Principles only with regard to data economy scenarios.

These Principles do not address general legal doctrines such as those governing formation of contracts or protections provided to consumers in consumer contracts, leaving those matters to existing law. Thus, these Principles do not differentiate between consumers and businesses as customers. Rather than create new protective doctrines unique to this context, these Principles provide guidance as to the application in a data setting of existing protective rules and doctrines, which often differentiate between consumers and businesses. Whenever these Principles refer to "contract" or "contractual," this automatically implies that all general contract law doctrines, whether from statute or common law, apply, and that, when the contracting parties are a business and a consumer, all applicable consumer protection standards remain unaffected. These doctrines and standards vary from jurisdiction to jurisdiction (e.g., notions of "unconscionability" and "unfairness" in business-to-business transactions may mean very different things in different jurisdictions), and it is not the purpose of these Principles to change, with regard to data, a more general approach taken by the contract law of a particular jurisdiction on these matters.

d. Relationship with property law. These Principles do not address whether rights in data are to be characterized as "ownership" or "property" (except, of course, when other law, such as intellectual property law or the like, affirmatively creates property rights), nor do they take any position in the controversy between more privacy-oriented and more property-oriented theories of data law. Rather, they describe the attributes of rights with regard to data without addressing the issue of "proper" doctrinal characterization as one or the other.

REPORTERS' NOTES

United States:

Paragraph (1) of this Principle is based on the structure of a number of "soft law" instruments. See, e.g., Int'l Inst. for the Unification of Priv. L., UNIDROIT Principles of International Commercial Contracts, Preamble (2016); Hague Principles on Choice of Law in International Commercial Contracts, Preamble (2015).

U.S. bodies of law that apply to matters also addressed in these Principles include most particularly contract law (see Restatement of the Law Second, Contracts (AM. L. INST. 1981)) and tort law (see Restatement of the Law Third, Torts: Liability for Economic Harm (AM. L. INST. 2020)). Contract law principles in Article 2 of the Uniform Commercial Code (UCC) do not apply directly to data transactions (because data does not constitute "goods" (see UCC §§ 2-102, 2-105 (2021-2022 ed.)), but can be a source of useful analogies. Principles that address security interests in data are also governed in the United States by Article 9 of the UCC.

U.S. bodies of law that can apply to data transactions, and to which these Principles defer, include data privacy law (see Principles of Law, Data Privacy (AM. L. INST. 2020)), copyright law (see 17 U.S.C.A. § 101 et seq. and Restatement of the Law, Copyright (AM. L. INST. forthcoming)), and property law (see Restatement of the Law Fourth, Property (AM. L. INST. forthcoming)).

For a thoughtful analysis of the need for special contract law for data transfers, see Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 662 (2019). For an analysis of establishing principles for data by analogy to other subjects, see Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863 (2019).

In the United States, see and compare paragraph (1) with, e.g., UCC § 1-103, which identifies underlying purposes and policies of the Uniform Commercial Code as (1) simplification, clarification, and modernization of the law governing commercial transactions, (2) permitting the continued expansion of commercial practices through custom, usage, and agreement of the parties, and (3) making uniform the law among various jurisdictions. As stated in Official Comment 1 to UCC § 1-103, the Uniform Commercial Code should be construed in accordance with its underlying purposes and policies. The text of each section should be read in light of the purpose and policy of the rule or principle in question, and also of the Uniform Commercial Code as a whole, and the application of language should be construed narrowly or broadly, as the case may be, in conformity with the purposes and policies involved.

As to whether rights in data are to be characterized as "ownership" or "property," the literature is extensive. See, e.g., Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1 (2018) ("The rationales for propertizing data are thus not compelling and are outweighed by the rationales for keeping the data 'open.' No new property rights need to be created for data."); Margaret Jane Radin, *A Comment on Information Propertization and Its Legal Milieu*, 54 CLEV. ST. L. REV. 23, 25 (2006) (noting that "Propertization of information not included in copyright has been significantly expanded through resurrection of a metamorphosed version of the common-law doctrine of trespass to chattels"); Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases*, 18 Berkeley Tech. L.J. 773, 787 (2003).

Of course, even discussing whether rights in data are to be characterized as property rights presupposes a common concept of what constitutes "property." Scholarship of the last few decades makes it clear that law has not settled on such a concept and, moreover, that the concept can have different meanings in different contexts. But "property is an artifact, a human creation that can be, and has been, modified in accordance with human needs and values." Hanoch Dagan, *The Craft of Property*, 91 CAL. L. REV. 1517, 1532 (2003).

For an extensive discussion of the nature of "property" and "ownership" in general, see Restatement of the Law Fourth, Property, Volume 1, Division I §§ 1-3 (AM. L. INST., Council Draft No. 1, 2019).

Europe:

a. Addressees and added value. As already pointed out in the U.S. Reporters' Notes, the structure of paragraph (1) of this Principle draws inspiration from internationally well-recognized "soft law" instruments such as Article 1:101 of the Principles of European Contract Law (PECL), the Preamble of the International Institute for the Unification of Private Law (UNIDROIT) Principles of International Commercial Contracts (2016), or the Introduction to the Hague Principles on Choice of Law in International Commercial Contracts (2015).

Paragraph (1) clarifies these Principles' intent to be sufficiently concrete to allow for the solution of a variety of legal problems "on the ground," and provide guidance for a broad variety of actors. Existing standards and frameworks have been an essential source of inspiration for these Principles. However, frameworks with a similarly broad scope, such as the UN Global Pulse Principles (United Nations Development Group, "Data Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda," 2017), the Organisation for Economic Co-operation and Development (OECD) Principles (OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 12), the OECD Recommendation (OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, 2021), the Principles formulated by the Danish Data Ethics Council (The Expert Group on Data Ethics, "Data for the Benefit of the People," 2018, p. 34), and the German Data Ethics Commission (Opinion of the Data Ethics Commission, 2019, p. 6 f.), as well as the principles put forward by the Finnish EU Presidency (Finland's Presidency of the Council of the European Union, Principles for a human-centric, thriving and balanced data economy, 2019), are on a higher level of abstraction and of a more aspirational nature, compared to these Principles.

More concrete are the "data strategies" that have been presented, e.g., by the European Commission (COM(2020) 66 final) and certain European states (e.g., Data Strategy of the United Kingdom, 2020; Data Strategy of the German Federal Government, Datenstrategie der Bundesregierung, 2021). Some states did not address their intentions to introduce comprehensive legal frameworks for the data economy in genuine "data strategies" but implemented them in their strategies on Artificial Intelligence (see the French AI Strategy: Villani Report, 2018, p. 20 ff). These strategies already formulate legislative measures that should be enacted in the future and thus provide an outlook on the possible legal landscape of the near future. However, they limit themselves to this outlook and do not yet contain any material proposals for legal acts.

Concrete guidance to parties who have decided to enter into a "data transaction" is achieved by the handful of existing model agreements for data transactions (see the "Report on collected model contract terms" by the Support Centre for Data Sharing, the Dutch vision on data sharing between businesses by the Dutch Ministry of Economic Affairs, or the "Danish model agreements for data transfers"). The most advanced initiative seems to be the "Contract Guidelines on Utilization of AI and Data – Data Section" published by the Japanese Ministry of Economy, Trade and Industry (METI) (METI, Contract Guidelines on Utilization of AI and Data – Data Section, 2018). However, model agreements cannot give guidance to courts or legislators as to whether parties must enter into negotiations about a transaction, pay damages to each other, etc. Compared to the listed principles, standards, and strategies, these Principles have a more comprehensive scope, as, on the one hand, they target various audiences, and, on the other hand, they aim to address a variety of different legal problems on a level of concreteness that allows solving legal problems "on the ground."

Finally, with the proposal for a Data Act (COM(2022) 68 final), there now exists an advanced legislative proposal at the European level that addresses several aspects of Data Transactions and Data Rights within the meaning of these Principles, including provisions on business-to-consumer (B2C) and business-to-business (B2B) data sharing, horizontal obligations for data holders legally obliged to make data available, and unfair terms related to data access and use between enterprises. While the proposed Data Act, which has been influenced by these Principles, widely overlaps with these Principles, its scope is more limited. For example, with regard to B2C and B2B data sharing, the Data Act only addresses data generated by connected products and virtual assistants. In contrast, Part III of these Principles applies to data generated by any means. Also, the Data Act does not contain any provisions on third-party effects of data activities as addressed by Part IV of these Principles nor on Multi-State Issues, which are addressed in Part V. By contrast, the Data Act addresses some issues, such as business-to-government (B2G) data sharing, that are not specifically addressed by these Principles.

b. Relationship with specific areas of the law not addressed by these Principles. The European Union has introduced several instruments that—either directly or indirectly—produce effects for the data economy, and thus also affect the subject matter of these Principles. Areas of law in which such instruments exist include data privacy/data protection law, copyright or other intellectual property law, and trade secrets law.

As far as personal data is concerned, it is in particular the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) that regulates the lawfulness of processing of personal data and data subjects' rights. In addition, the E-Privacy Directive (Directive 2002/58/EC) lays down rules for the processing of personal data in the electronic communication sector. The latter should already have been replaced by a new Regulation some years ago (cf. Commission Proposal COM(2017), 10 final), which recently reached the stage of trilogue.

In the field of intellectual property, there are numerous instruments on an EU level that may also cover data. Of particular relevance for the data economy are the Database Directive (Directive 96/9/EC), the Information Society Services Directive (Directive 2001/29/EC), and the Copyright DSM Directive (Directive (EU) 2019/790). But data may also be covered by more specific regimes,

such as the Software Directive (Directive 2009/24/EC). Finally, data are protected under the Trade Secrets Directive (Directive (EU) 2016/943) against unlawful acquisition, use, and disclosure.

c. Relationship with contract rules and doctrines. The relationship between provisions of European civil codes that have inspired and guided these Principles, or that serve as the basis for analogies, are discussed at length in the Reporters' Notes to the Principles in Part II. Basic contract law doctrines, such as on the formation, nullity, and validity of a contract, are not only excluded by these Principles, but are left to national law even by comprehensive EU contract law regimes. Even the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770), which is the most advanced European piece of legislation on data contracts, leaves this issue to the applicable national law (see Article 3(10) DCSD).

d. Relationship with property law. Whether to introduce a "data ownership" right was the subject of intensive debate from a policy point of view. While the European Commission considered introducing a "data producer's right" at the EU level in its Communication on "Building a European Data Economy" (COM(2017) 9 final, p. 10 ff), it changed its position after severe criticism that the introduction of such a new intellectual property right could be detrimental to the data economy. Currently, the predominant view in Europe seems to be that access rights and similar data rights are more promising as a way forward than data ownership rights (COM(2020) 66 final p. 4 ff.; COM(2018) 232 final, p. 9). For more detailed elaborations, see the Reporters' Notes to Principle 16.

Principle 2. Scope of these Principles

(1) The primary focus of these Principles is on records of large quantities of information as an asset, resource, or tradeable commodity. These Principles do not address functional data, i.e., data the main purpose of which is to deliver particular functionalities (such as a computer program), and representative data, i.e., data the main purpose of which is to represent other assets or value (such as crypto-assets).

(2) Subject to paragraph (3), these Principles address:

(a) data contracts,

(b) data rights, and

(c) third-party aspects of data contracts and data rights.

(3) These Principles are not designed to apply to public bodies insofar as such bodies are engaging in the exercise of sovereign powers.

Comment:

a. Focus on information. The definition of "data" in Principle 3(1)(a) is broad. Applying these Principles to all rights and transactions about data (as so defined) would result in application of these Principles beyond their intended context. These Principles (as well as the terms "data

contracts," "data rights," etc.) should be understood as covering only issues that have a primary focus on records of large quantities of information. They should not cover cases in which, e.g., the focus is on the medium itself, or on an entirely different aspect of data. This flexible approach allows for these Principles to be applied to the whole transaction, to be applied to a particular part or aspect of a transaction, or to not be applied at all when the "records of information" aspect is not the focus of the subject matter.

Illustration:

3. A simple contract between a law firm and a client pursuant to which the law firm will represent the client in contract negotiations is not within the scope of these Principles even when it is anticipated that the law firm will transmit proposed drafts of transactional documents in digital form through an electronic message system. This is because the focus of the contract between the law firm and the client is not on the records of information, but rather the legal advice as such. Of course, a wider relationship between a law firm and a client may include aspects that are within the scope of these Principles, and that relationship may include, e.g., access to data or processing of data within the meaning of these Principles.

The distinction between a primary focus on records of (large quantities of) information and a different focus is particularly relevant when it comes to digital phenomena that are not primarily considered as "data" even though, technically speaking, they have the same or a very similar nature. A computer program, for example, is primarily seen as a set of commands delivering particular functionalities ("functional data"). Cryptocurrencies and other tokens may be seen as, among other things, data packets, but clearly the focus is not on any value inherent in the information recorded in the tokens, but rather on the off-ledger asset represented by them ("representative data") or the on-ledger asset generated by the fact that other members of a community are prepared to trade them for value. This is why paragraph (1) of this Principle clarifies that these Principles do not address functional data or representative data.

Illustration:

4. A transfer of Bitcoins (a form of cryptocurrency) from wallet holder A to wallet holder B is not a "data transaction" for purposes of these Principles because the transaction is primarily about a transfer of value represented by a virtual token and documented on the

blockchain. Likewise, in-game purchase of a weapon or superpower would not be a "data transaction" and would not be covered by these Principles because the focus is on the functionality, not on the information.

The fact that a set of digital data normally serves the purpose of delivering certain functionalities does not exclude the possibility that the same set of data may also be used without reference to those functionalities, in which case the data could be within the scope of these Principles.

b. Asset, resource, or tradeable commodity. Information has always been subject to a variety of different contracts, in particular service contracts, and information rights have always been included in a wide range of legal regimes. Many of these issues fall outside the scope of these Principles already because they are not about "digital" data, or because the information is not the focus of the transaction. However, there are cases in which the law provides that, e.g., particular information must be given to a consumer with particular digital means, or in which two parties agree in a contract that one party will disclose and publish all its conflicts of interest on the party's website. In these cases, the legal rules are about digital data, and they are about the information aspect, but they still are not within the focus of these Principles. This is because these Principles are not primarily concerned with single pieces of information provided with the aim of immediately letting another party *know* something, but more about "bulk" or "serial" data, usually to be processed with the help of machines, and used as an asset, resource, or tradeable commodity. Accordingly, supplying data within the meaning of these Principles is not so much about *doing* something, but more about *delivering* something.

c. Issues addressed. The development and identification of clear and certain principles that promote a data economy that is both efficient and fair is of fundamental importance to the development of that economy. Law governs the data economy in a wide variety of ways. These include the allocation of private rights with respect to transactions and the data to which the transactions relate, unfair competition and antitrust law, privacy and data protection law, etc. These Principles do not address that entire range of legal issues but, rather, focus on data contracts and data rights, and on the third-party aspects of such contracts and rights, as far as these are relevant in the context. In addition, these Principles provide some limited guidance as to multi-state issues with regard to data contracts and data rights, without providing a full set of choice-of-law rules.

d. Public bodies. The control and processing of data by public bodies in the exercise of sovereign powers afforded to them by the applicable law is an extremely important topic that is, however, beyond the boundaries of these Principles. These Principles therefore apply only to the extent that exercise of sovereign powers is not implicated (but even when these Principles could be applied to activities of public bodies, other, more specific, rules for dealings with the government or government agencies may also apply).

Illustration:

5. A public prosecutor collects data on a group of individuals suspected of having committed cybercrimes. This activity is one in the exercise of sovereign powers, and suspects might not, e.g., rely on any of the Principles concerning data rights in co-generated data. However, if that authority enters into a contract with a private company for data analytics services, these Principles might apply, because the authority would not exercise any sovereign powers vis-à-vis that company.

References to a "public body" in these Principles include public administrations and judges as well as civil law notaries and any kind of body insofar as such bodies are engaging in the exercise of sovereign powers, be it directly or by means of delegation to any other authorities, official professionals, or mixed bodies.

Even though these Principles do not apply to public bodies insofar as such bodies are engaging in the exercise of sovereign powers, these Principles may still apply to situations in which public bodies have collected data in the exercise of sovereign powers, but are now making that data available under schemes of open public sector data and the like, because sharing data in that manner is not in itself exercise of sovereign powers.

REPORTERS' NOTES

United States:

As to the limitation of the scope of these Principles to "digital data," see the definition of "digital database" in the Principles of the Law, Software Contracts (AM. L. INST. 2010). The first sentence of that definition states that a "digital database" is "a compilation of facts arranged in a systematic manner and stored electronically." Principles of the Law, Software Contracts § 1.01(f)(2) (AM. L. INST. 2010).

U.S. bodies of law with related scope include the Model Computer Information Transactions Act (last revised or amended 2002) and the Principles of the Law, Software Contracts (AM. L. INST. 2010).

Contracts for the sale of goods are governed by Article 2 of the Uniform Commercial Code (UCC) (2021-2022 ed.), and contracts for the lease of goods are governed by UCC Article 2A. Courts have, on occasion, applied UCC Article 2 by analogy to transactions outside its formal scope, such as data and software contracts. See, e.g., Arbitron, Inc. v. Tralyn Broad., Inc., 400 F.3d 130, 138 & n.2 (2d Cir. 2005); i.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002). See generally Murray, *Under the Spreading Analogy of Article 2 of the Uniform Commercial Code*, 39 FORD. L. REV. 447 (1971).

Quite a few U.S. legal regimes address specific subsets of the data economy. See, e.g., Health Insurance Portability and Accountability Act, Pub. L. 104–191, Aug. 21, 1996, 110 Stat. 1936; California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West).

Europe:

a. Focus on information. The explicit reference to the focus on information in the scope of these Principles is unique from a European point of view. The same holds true for the terms "representative data" and "functional data" in paragraph (1), which are not defined at the EU level. However, since the term "representative data" also covers crypto-assets, there are certain overlaps with existing definitions of "virtual currencies," which are defined as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority" (see Article 1(2)(d) Directive (EU) 2018/843). The term "functional data" reflects the basic understanding in software engineering that a distinction must be made between the binary code of a computer program and other or "mere" data. The digital data that make up a computer program are characterized by the property that they enable computer hardware to perform computational or control functions (see Institute of Electrical and Electronics Engineers (IEEE), IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990). That computer programs perform a control function is also recognized by EU law (see Recital 10 of Directive 2009/24/EC).

Even though the explicit scope of these Principles is unique, it is clear from the subject matter that some legislations (implicitly) have the same focus. This is true for the Data Governance Act (DGA) (Regulation (EU) 2022/868), which wants to improve the conditions for data sharing in the internal market and, e.g., lays down a notification and supervisory framework for the provision of data intermediation services (Articles 10 ff DGA). However, "functional" and "representative data"—as used in paragraph (1)—are not explicitly excluded from its scope of application. And the definition of "data" as "digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording" (Article 2(1) DGA) may be too broad to ensure that the DGA does not apply to data that does not have a primary focus on information. It can, for example, be argued that a bitcoin is the digital representation of facts and information, namely the value, time, and recipient of a transaction.

The broad definition of "digital content" in Article 2(1) of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) covers functional data within the meaning of paragraph (1) as well as digital data when the primary focus is on records of large quantities of information as an asset, resource, or tradeable commodity. However, contrary to these Principles, the primary focus of the Directive is not on information, but on the functional level of data. Digital

representations of value such as electronic vouchers, e-coupons, or cryptocurrencies, i.e., representative data, are also explicitly not covered by the DCSD (Recital 23 DCSD).

b. Asset, resource, or tradeable commodity. EU instruments are typically not limited to large quantities of data with a primary focus on information. The General Data Protection Regulation (GDPR), for example, applies to the processing of personal data, which Article 4(1) defines "as any information relating to an identified or identifiable natural person." The Free Flow of Data Regulation (Regulation (EU) 2018/1807) refers to Article 4(1) of the GDPR to define non-personal data, and thus does not exclude single pieces of information provided with the aim of immediately letting another party know something.

d. Public bodies. European legislations on data oftentimes exclude public bodies acting in the exercise of their sovereign powers from the scope of application and vice versa. For example, the Open Data Directive (Directive (EU) 2019/1024) is addressed to public bodies, and excludes documents, the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned, from the scope of application (Article 1(2)(a) Open Data Directive). It is in a similar vein that paragraph (3) of this Principle does not apply to public bodies insofar as such bodies are engaging in the exercise of sovereign powers. For guidance as how to interpret paragraph (3), see Article 1 of the Brussels Ia Regulation (Regulation (EU) No 1215/2012), which contains a similar public–private law division and only applies when the public authority acts in the exercise of its public powers (CJEU Case C-645/11 para 33 – Sapir et al).

Principle 3. Definitions

(1) For the purposes of these Principles, the following definitions apply:

(a) "Data" means information recorded in any machine-readable format suitable for automated processing, stored in any medium or as it is being transmitted.

(b) "Copy" means any physical manifestation of data in any form or medium.

(c) "Processing data" means any operation or set of operations that is performed on data, whether or not by automated means; it includes, inter alia, the structuring, alteration, storage, retrieval, transmission, combination, aggregation, or erasure of data.

(d) "Access to data" means being in a position to read the data and utilize it, with or without having control of that data.

(e) "Control of data" means being in a position to access the data and determine the purposes and means of its processing.

(f) "Controller" means the person that, alone or jointly with other persons, has control of data.

(g) "Processor" means a person that, without being a controller, processes data on a controller's behalf.

(h) "Co-generated data" means data to the generation of which a person other than the controller has contributed, such as by being the subject of the information or the owner or operator of that subject, by pursuing a data-generating activity or owning or operating a data-generating device, or by producing or developing a data-generating product or service.

(i) "Derived data" means data generated by processing other data, and includes aggregated data and data inferred from other data with the help of external decision rules.

(j) "Data contract" means a contract the subject of which is data.

(k) "Data right" means a right against a controller of data that is specific to the nature of data and that arises from the way the data is generated, or from the law for reasons of public interest.

(l) "Data activities" means activities by a person with respect to data, such as collection, acquisition, control, processing, and other activities including onward supply of data.

(m) "Supply" of data means providing access to data to another person or putting another person in control of data.

(n) "Supplier" of data means a party who supplies data to another party, or undertakes to do so.

(o) "Recipient" of data means a party to whom data is supplied, or is to be supplied.

(p) "Transfer" of data means supply of data by way of which the supplier puts the recipient in control of the data, whether or not the supplier retains control of the data.

(q) "Porting" data means initiating the transfer of data controlled by another party to oneself or to a designated third party.

(r) "Erasure" of data means taking steps to ensure, as far as is reasonably possible, that the data is permanently inaccessible or otherwise unreadable.

(s) "Notice" means having knowledge of a fact or, from all the facts and circumstances of which a person has knowledge, being in a position that the person can reasonably be expected to have known of the fact.

(2) The terms "contract for the transfer of data," "contract for simple access to data," "contract for exploitation of a data source," "contract for authorization to access data," "contract for data pooling," "contract for the processing of data," "data trust contract," "data escrow contract," and "data marketplace contract," and any terms denoting the parties to such contracts, have the meanings given to them in Principles 7 to 15.

(3) References to a "person" include natural and legal persons, private or public. References to an "operation" or "activity" include operations or activities carried out with the help of other persons or of machines, including any artificial intelligence.

Comment:

a. "Data" and "copy." These Principles are concerned only with data that is in a machine-readable format suitable for automated processing. In common parlance, such data is often referred to as "digital" data. However, these Principles are intended to cover also nondigital technologies (such as analog computing and, perhaps, quantum computing) when those technologies enable comparable sorts of operations to be performed on the data by automated means, i.e., when data is recorded in other machine-readable formats suitable for automated processing. The intent, however, is to cover only data that is immediately suitable for automated processing by machines, not data that can be made suitable for such processing only by means of intervening technologies such as document scanners, or by similar technical means.

Illustration:

6. Company N runs a news website. N collects a wide range of data concerning the search requests and browsing habits of its visitors and records this data electronically. This data falls within the definition of "data" in paragraph (1)(a) of this Principle.

Thus, as used in these Principles, "data" would not cover the content of paper files even though that content can be made suitable for automated processing by way of a scanner and appropriate software. However, these Principles may also be appropriate for application by analogy to other recorded information in some circumstances depending on, inter alia, the way the information is recorded and the manner in which it is to be used.

Illustrations:

7. Business B has maintained many years of historical business records, which are recorded on charts printed on paper. Because those charts are not immediately suitable for automated processing, these Principles do not address matters with regard to this sort of data. If, however, the charts were scanned and the resulting data was stored in machine-readable format, these Principles would address matters with regard to the data.

8. Employee E of business B (unlawfully) "sells" B's customer database to competitor C. However, due to specific information-technology security measures taken by B, it is easier for E to print the customer data on paper to deliver to C than to store the information on a digital medium or transmit it online to C. C will immediately scan the prints and convert the data into a digital format. In a setting like this, it would not seem appropriate to restrict the application of these Principles—such as the Principles on unauthorized access and what it means for a downstream recipient—to the phases when the customer data is in digital format. (Note that issues of criminal and other liability on the part of E are beyond the scope of these Principles).

The term "data" has multiple facets in common parlance. In fact, lawyers frequently talk past each other when using the term because they are referring to different facets or concepts of "data." Much confusion has been caused, in particular, by the varying use of the terms "information" on the one hand and "data" on the other. These Principles use "data" to refer to information recorded in any form or medium, or to information in a state of transmission. In the case of digital data, this means that data is more than the binary electrical impulse stored or being transmitted, as it includes context and semantics. Context and semantics are to be found in metadata, domain tables, etc.

The term "data" as defined in paragraph (1)(a) has more than one layer. Apart from the semantic layer, i.e., the layer that constitutes meaning, it can be understood as referring to the code as such (e.g., a characteristic binary string of "0s" and "1s") or its physical manifestation on a particular medium. The former can be "coded," "modified," "decompiled," etc., while the latter can be "stored," "damaged," "erased," etc. In order to make this distinction more transparent, these Principles restrict the term "data" to the former, i.e., to the code as such (including context and semantics), while the physical manifestation on a medium is called a "copy." A term that is often

used with a similar meaning is "file," which, however, seems also to have some associations that are not intended in this context.

Illustration:

9. Business B collects data concerning B's transactions with its customers, such as A, on a local hard disk drive, but there is a backup on a cloud server provided by C. The fact that A has bought a specified commodity from B on a specified date is the information. This information is recorded in the form of coded binary impulses, i.e., a characteristic string of "0s" and "1s," which constitutes the data. This string can be found as a physical manifestation both on B's local hard disk drive and on C's cloud server, so there exist two copies of the data (or even more, as there will be redundancies, and as there may be transitional copies in the cache of several devices).

The definition of the term "copy" applies only as the term is used in these Principles. The definition here is not intended to resolve issues about the meaning of that term in other areas of the law, such as copyright law.

b. "Processing data" and "access to data." A central term is "processing data," which is defined to include any operation or set of operations that is performed on data. Thus "processing" includes operations such as organizing, structuring, storing, adapting or altering, retrieving, transmitting, aligning or combining, restricting, erasing, or destroying data. Some of these operations directly target the data as such, while others target the data only indirectly by targeting one or all existing copies. Defining the term generically to cover all of these operations is useful because, given the multitude of different ways in which data can be handled or used, it would be quite unwieldy to utilize different terminology for each of them, and, given the pace at which technology is developing, any terminology defined today may be incomplete or inappropriate tomorrow.

"Access to data" and processing of data are closely related notions. "Access" means being in a position to read the data and utilize it, in unspecified or specified ways, and with or without having control of that data. Processing of data usually requires access to the data. Access, conversely, often includes some kind of processing, but not necessarily so; merely reading data on a screen would amount to access but normally not to processing, at least not in the narrower sense adopted by these Principles.

Illustration:

10. Business B in Illustration no. 9 processes transactional data by structuring it, by analyzing it, and by way of many other operations. Assuming B checks its transactions with A because A has filed a complaint (e.g., A claims never to have received a commodity for which he has been billed), retrieving transactional data from either the local drive or the cloud and making it visible on a screen on one of B's devices amounts to processing (and a form of accessing). If B lets A look at the screen and read the information about A's shopping history, access (on the part of A) is not accompanied by processing.

c. "Control of data," "controller," and "processor." Another central notion is that of "control of data." "Control of data" means being in a position to access the data and to determine the purposes and means of its processing, with or without having a right to do so. A "controller" means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, has control of data.

Illustration:

11. Business B in Illustration no. 9 has its business data stored in cloud space on servers operated by C. B has the access credentials required to access and process the data as B deems appropriate. Even though B is not in "physical" control of the medium, B has, for the purposes of these Principles, control of the data and qualifies as a controller. C does not qualify as a controller insofar as there are features in place, be they of a technical or legal nature, that prevent C from determining the processing of its customers' data.

Control does not necessarily mean being in a position to determine any possible kind of processing, e.g., a person may have access to a set of data and may be in a position to transfer it to someone else, but the data may be protected against modification. Also, "control" does not necessarily imply that the "controller" actually seeks access to the data or has the technical capabilities that are necessary for actually accessing the data, as long as there are technical or legal features that would allow that party, without unreasonable effort, to access the data if the party wished to do so.

Illustration:

12. Company N runs a news website. Use of the website by each visitor is, with the consent of N, closely monitored and recorded by data broker B (B paying a remuneration

to N). While company N itself never takes an interest in collecting the visitors' data, and may not even have made any technical arrangements that would allow such collection, it would not require unreasonable effort on N's part to do so. N therefore has control of the visitors' data because it could access the data at any time if it so wished and because N determines the means and purposes of their processing by allowing B to harvest the data.

Frequently, controllers enter into contractual arrangements with other persons about the processing of data to be carried out by those other persons, while keeping full control because processing is carried out on the controllers' behalf and according to their directions. Such other persons are processors, which means that, in some contexts—such as when it comes to the question of whose position primarily counts for rightfulness under Principle 28—it is the controller on whose behalf the processor is acting that counts. Being a processor and processing data on behalf of a controller does not constitute control of data, so the roles of "processor" and of "controller" are normally mutually exclusive.

Illustrations:

13. Business B decides to outsource payroll services with regard to B's employees and hires company P to perform these services. For this purpose, relevant data (such as the employees' names, wages, bank accounts, or tax numbers) is processed by P on B's behalf. P is not free to determine the means and, in particular, the purposes, for which the employee data is processed, but rather has to follow B's directions. P is therefore not a controller, but a processor.

14. Business B allows financial consulting firm A to access B's business data in order to analyze B's business situation. A is not entirely free to determine the means and the purposes of processing B's business data (e.g., A would not be allowed to disclose the data to B's competitors), which could mean A is only a processor. However, A is not strictly subject to B's directions either (e.g., B would not be allowed to direct A that A ignore certain data in order to paint a more optimistic picture of B's business situation than is the reality). Therefore, it is more convincing to qualify A as controller, albeit as a controller that is subject to quite rigid restrictions when it comes to the purposes of the processing.

Employees or similar persons integrated in the controller's organizational framework and through whom the controller exercises control would not even be considered "processors." When

the controller is a legal entity, it can act only through its employees and other agents. Accordingly, when an employee is merely executing decisions made by the employer, any activity of the employee with regard to data should be attributed exclusively to the employer.

d. "Co-generated data" and "derived data." "Co-generated data" means data to the generation of which a person has contributed, such as by being the subject of the information or the owner or operator of that subject, by pursuing a data-generating activity or owning or operating a data-generating device, or by producing or developing a data-generating product or service. The term is used in the context of a particular type of data rights dealt with under Part III, Chapter B. The term is designed to indicate that, usually, a number of different persons have contributed to the generation of data, sometimes in very different roles. There may be situations in which only one person has contributed, at least in a meaningful way, to the generation of data. In those situations, the term "co-generated" may not be fully appropriate, but such a person would (*a fortiori*) have the rights under Part III, Chapter B.

While the term "co-generated data" refers to the parties who had a share in the generation of data, the term "derived data" refers to the fact that data develops in a dynamic way and is often generated on the basis of other data. Only an exact copy of a particular set of data would count as the "same" data, and even minor modifications would make a set of data a "different" set of data. In these Principles, "derived data" means any data that the relevant controller has generated by processing other data, i.e., by modifying, reducing, or extrapolating other data, or drawing inferences from other data. Given that there are many different ways in which data can be generated on the basis of other data, and that it is so difficult to draw a clear line and provide a coherent and complete set of classifications, these Principles adopt a broad notion of "derived." In particular, they do not differentiate between "derived" and "inferred" data (i.e., data generated from other data with the help of external decision rules).

Illustration:

15. When opening a user account for an online game run by business G, users provide to G their name, email address, and credit card data, and G collects all sorts of other user data, such as about the user's gaming behavior, typing pace, etc. G then restructures the data, fills gaps in the data, and infers, with the help of algorithms and other knowledge not contained in the collected data, new information from the user data, e.g., predictions

about a party's disposition to suffer from depression. The restructured data, the completed data, and the data on potential depression all count as derived data.

e. "Data contracts," "data rights," and "data activities." These Principles are about data contracts and data rights, so these two terms are important for the proper understanding of these Principles. Both terms are to be understood broadly. A "data contract" is a contract the subject of which is data, either in the sense that data is the object of the transaction between two parties (i.e., the data is to be transferred, disclosed, otherwise shared, etc.) or in the sense that one party promises to do something with regard to the data (i.e., the data is to be collected, processed, secured, etc.).

A "data right" means a right against a controller of certain data that is specific to the nature of data as a non-rivalrous resource and that arises from the way the data is generated (see Principles 18 to 23), or from the law for reasons of public interest (see Principles 24 to 27). It may, in particular, be a right to access to or porting of the data, to correction of the data or desistance from data use, or, very exceptionally, to an economic share in profits derived from using the data. Data rights are, in a certain way, the data-specific corollary to the ownership rights found in the tangible world or with regard to intellectual property.

"Data activities" is a term referred to in various places in these Principles, in particular in Part IV with regard to affected third parties. It means any activities by a person with respect to data, such as collection, acquisition, control, processing, and other activities, including onward supply of data. The term is to be understood broadly, and as comprising activities of a factual nature (e.g., actually disclosing data to another party) as well as of a legal nature (e.g., making a contract with another party about access to data).

f. "Supply," "supplier," and "recipient." It is in particular in data contracts that "supply" of data comes into play. The person who supplies data is the "supplier" and the other person is the "recipient." "Supply" of data should be understood very broadly. In particular, it is sufficient that the recipient gains access to the data, while it is not necessary that the recipient also gains control.

Illustrations:

16. Company N runs a news website offering any visitor access—without a paywall—to world news. N collects a wide range of data concerning the search requests and browsing habits of its visitors and "sells" and transfers the data to business B, which will use the data for profiling and scoring purposes. N and B agree that the data will be

transferred to one of B's servers. This transfer of the data to B qualifies as "supply" of the visitor data.

17. Assume that company N in Illustration no. 16 does not collect the visitors' data itself but instead allows B to collect the data on N's site. Despite the fact that N does not physically transmit any data to B, N still enables B to access the data, and to gain control of the data, and therefore qualifies as a "supplier" under these Principles.

g. "Transfer," "porting," and "erasure." While "supply" of data is a very broad and rather generic term, it is often necessary to be more specific and to differentiate between different types of supply. An important type of supply is "transfer" of data, in which the supplier puts the recipient in control of the data supplied (as contrasted with simple access). This normally implies that data is to be physically stored on a medium within the recipient's sphere of control. Note that "transfer" does not imply that copies of the data are subsequently erased by the supplier.

Illustration:

18. The supply of data to B in both Illustration nos. 16 and 17 is a "transfer" as the data is supplied to B's servers, which grants B full control of the data.

"Porting" data, which is frequently also referred to as "portability" of data, means requesting or otherwise initiating the transfer of data controlled by another party to oneself or to a particular third party. "Porting" and "transfer" are thus closely related, with the main difference being that of perspective, as "porting" clearly takes the perspective of the recipient exercising a right, while "transfer" is more neutral and describes an activity of the supplier. "Porting" tends to suggest to a certain extent that the person requesting the transfer has a data right, i.e., that the data is, in one way or another, that person's data.

Illustration:

19. Supply of the data collected by N to B in Illustration no. 16 would be described as a "transfer" (and not as "porting") because it is supplier N who collects the data and who then initiates transfer to B. However, if B is allowed to harvest data from the site in Illustration no. 17 and store the harvested data on B's own medium, that would be described as "porting" rather than as "transfer," because the active part is played by recipient B.

In particular contexts, "erasure" of data (one type of "processing" data) may become relevant. This means taking reasonable steps to ensure that the data is permanently inaccessible or otherwise unreadable. What counts as "reasonable" depends on the individual circumstances and the purposes of erasure. It may, in an individual case, mean deleting all copies of the data that are accessible to the person erasing the data, and, as far as possible, deleting all copies accessible to third parties to whom that person has supplied the data. This is because, given the nature of data, there may exist an indefinite number of copies worldwide. Sometimes it may be sufficient to press a "delete" button even though, strictly speaking, the data would then still remain to be retrievable until the relevant storage space has been fully overwritten, and possibly even after that point. But normally, more sophisticated technical measures would be required.

h. Notice. A term that is used throughout these Principles is "notice." "Notice" means having knowledge of a fact, but also covers situations in which, from all the facts and circumstances of which a person has knowledge, the person can reasonably be expected to have known of the fact. It includes what is often referred to as "willful blindness." If a person has notice of a fact (e.g., of the fact that processing data was wrongful), that often gives rise to an expectation that the person take action or desist from particular actions accordingly, and if the person fails to react as can reasonably be expected, this often triggers adverse legal consequences.

i. Definitions in other Principles. Paragraph (2) reminds us that the only terms defined in this Principle are those used throughout these Principles. There are other terms that require a definition but that are used only in one Principle, or in one specific context, and are thus better defined in the relevant context; in particular, the different types of data transactions identified in Part II.

j. References to "person," "operation," or "activity." Paragraph (3) clarifies that reference to "person" includes any natural or legal person, or group of persons. What may be more important is that reference to any "operation" or "activity" includes operations and activities carried out by human auxiliaries and, increasingly, by machines. Machines include any artificial intelligence, i.e., it is irrelevant for the application of these Principles whether, e.g., a data contract was concluded by way of two individuals exchanging offer and acceptance or whether offer and acceptance were articulated and received by "autonomous" software agents.

When a contract is concluded by machines, some concepts used in these Principles may require adaptation. For example, these Principles frequently refer to a party having "notice" of a

fact. When there is not a human but a machine that carries out relevant operations or activities, the concept of "notice" may have to be adapted.

Illustration:

20. A contract for the transfer of particular data is made with the help of two different autonomous software agents operated by supplier S and recipient R. S had received the data from third party T under another contract, and under that contract S had promised not to forward or disclose the data to any other person. According to Principle 34, T may have remedies against R if R had "knowledge" or could be expected to have knowledge of S's breach vis-à-vis T and further conditions are met. If R used an autonomous software agent and that agent was unable to process information as to restrictions of that kind, R cannot hide behind the agent and claim to have acted in good faith.

Equally, any reference to intent or to standards of care, due diligence, etc. may have to be understood in a way that is suitable for machine-to-machine dealings. However, this is not in any way different from machine-to-machine dealings other than in the context of data rights and transactions, which is why these Principles do not spell out in detail how general concepts are to be adapted.

REPORTERS' NOTES

United States:

The definitions presented in this Principle are "internal" in the sense that they do not begin with the defined terms and then attempt to identify their "true" or essential meaning. Rather, the defined terms are more in the nature of abbreviations for broader concepts; in that context, it is not the abbreviation (the defined term) itself that is important but, rather, it is the definition (the broader concept) that is key. Nonetheless, inasmuch as readers cannot be expected to constantly refer to the definitions in this or any other complex set of proposed rules, it is certainly desirable that the defined terms convey a sense that is consistent with their definitions.

While these Principles are not themselves statutory in nature, they may serve as the basis for future legislation. If so, the definitions presented here can serve as the basis of the definitional provisions in such legislation.

Nomenclature concerning "data" and "information" is not standardized in the United States. "In everyday parlance, the terms "data" and "information" are often used synonymously." Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1 (2018). Legal distinctions between the terms are often indistinct. For example, Black's Law Dictionary defines "datum" (the singular of "data")

as "a piece of information." *Datum*, BLACK'S LAW DICTIONARY (11th ed. 2019). The federal Electronic Signatures in Global and National Commerce Act and the Uniform Electronic Transactions Act define "information" as "data, text, images, sounds, codes, computer programs, software, databases, or the like." 15 U.S.C. § 7006(7); Uniform Electronic Transactions Act § 2(10) (1999). They do not, however, define "data." The same is true of the Model Computer Information Transactions Act (MCITA) (last revised or amended 2002) originally promulgated as the Uniform Computer Information Transactions Act. See MCITA § 102(a)(35) (defining "information" as "data, text, images, sounds, mask works, or computer programs, including collections and compilations of them").

With respect to "copy," see MCITA § 102(a)(20) ("'copy' means the medium on which information is fixed on a temporary or permanent basis and from which it can be perceived, reproduced, used, or communicated, either directly or with the aid of a machine or device.")

With respect to "digital data," see the definition of "electronic" in Principles of the Law, Software Contracts § 1.01(h) (AM. L. INST. 2010) ("'Electronic' means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities").

Europe:

a. "Data" and *"copy."* The definitions of "data" used in Europe vary significantly depending on the context and the respective scientific field. In the context of the data economy, the computer science understanding of data as (machine-readable) representation of information seems to be gaining general acceptance (e.g., United Nations Commission on International Trade Law (UNICITRAL), Legal issues related to the digital economy – data transactions (2020) p. 2 f; Herbert Zech, "Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt', 2015 *Gewerblicher Rechtsschutz und Urheberrecht*, p. 1151, 1153; Thomas Streinz, 'The Evolution of European Data Law' available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971). One of the most frequently cited definitions in that regard is the one suggested by International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 2382:2015, according to which data is "a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing." The computer science understanding has also been picked up by the European Commission. The Data Governance Act (DGA) (see Article 2(1) DGA, Regulation (EU) 2022/868), the Digital Markets Act (see Article 2(24) ST 8722/2022 INIT), as well as the recent proposal for a Data Act (see Article 2(1) COM(2022) 68 final) define "data" as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording." In contrast, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) defines "personal data" in Article 4(1) as "any information relating to an identified or identifiable natural person." While these Principles follow the general trend of defining "data" as machine-readable representation of information, they deviate from the ISO definition. In light of the many terms in this definition that tend to raise difficult questions of interpretation themselves (e.g., "formalized," "suitable for") and of the trend toward a broader and more encompassing notion of "processing," these Principles

adopt a simpler definition, inspired by the definition chosen by the ALI in the Principles of the Law, Data Privacy (AM. L. INST. 2020).

The definition of "copy" in these Principles as physical manifestation of data differs slightly from the understanding of the term in EU law. In EU law, the term "copy" is often used to refer to an identical data set (see Articles 13(1)(f), 14(1)(f), 15(4) GDPR; Articles 3(2), 6 Copyright Directive, Directive (EU) 2019/790). This understanding of the noun corresponds in essence with the ISO/IEC 2382:2015 definition of the verb "copy" as to "read data from a source data medium, leaving the source data unchanged, and to write the same data on a destination data medium that may differ from that of the source." In the Institute of Electrical and Electronics Engineers (IEEE) standard glossary "copy" is defined as: "To read data from a source, leaving the source data unchanged, and to write the same data elsewhere in a physical form that may differ from that of the source. For example, to copy data from a magnetic disk onto a magnetic tape." Paragraph (1)(b) of this Principle does not deviate in substance from these definitions, but rather stresses the fact that, when identical data sets are stored in different places, there are two or more physical manifestations on a medium.

b. "Processing data" and "access to data." The definition of "processing" in these Principles is not entirely identical with the definition under EU law, notably the definition in the GDPR and the Data Act proposal. Article 3(2) of the GDPR and Article 2(11) of the Data Act proposal define "processing" as any "operation or set of operations which is performed on (personal) data or on sets of (personal) data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Activities, such as mere viewing, or disclosure as such, without any "physical" operation, such as the generation of transitional copies, can undoubtedly infringe a person's privacy and thus fall under the GDPR's definition of "processing." However, those activities are performed only on an intellectual level and include no actual operation that is performed on the data. Hence, these Principles suggest that in the context of the data economy the term 'processing' should not cover the mere viewing of data. The current Data Act proposal has borrowed the definition of "processing" from the GDPR (except that it is referred to as data instead of *personal* data), which would suggest a broader understanding of processing.

The Data Governance Act (DGA) (Regulation (EU) 2022/868) is the first EU instrument to introduce a definition for "access." According to Article 2(13), "access means processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organizational requirements, without necessarily implying the transmission or downloading of such data." In essence, this definition coincides with these Principles' understanding of the term.

The term "access" is also used in several sector-specific regimes, e.g., Articles 61 to 66 of the Type Approval Regulation (Regulation (EU) 2018/858); Article 36 and 66 f of the Payment Sector Directive II (PSD II) (Directive (EU) 2015/2366); several times in the Electricity Directive (Directive (EU) 2019/944) and in Article 17 of the Infrastructure for Spatial Information in the European Community (INSPIRE) Directive (Directive 2007/2/EC), which grant parties access to certain sets of data. These rights are frequently referred to as "data access rights" (e.g., COM(2020)

66 final, p. 12). However, a clear terminology that distinguishes between data portability—a term used in Art 20 GDPR (see the Reporters' Notes to Principle 24)—and data access has not been established. Therefore, the label "data access right" does not necessarily imply that it gives a party less extensive rights than a portability right.

c. "Control of data," "controller," and "processor." In Article 4(7) of the GDPR, a "controller" is defined as natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. To an increasing extent, the term is used also with regard to non-personal data (see, e.g., Global Partnership on AI, A Framework Paper for GPAI's work on Data Governance, 2020). The DGA uses the term "data holder," which is defined as a "legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control" in Article 2(8). The definition of a "data holder" in the Data Act proposal is slightly different from the DGA. According to Article 2(6), a data holder is the legal or natural person who has the rights or obligations under the Data Act proposal or any other Union or national legislation implementing Union law. Additionally, a data holder is also the natural or legal person that is in the position to make available certain non-personal data through control of the technical design of the product and related service. These Principles have opted to follow this trend and thus use the same term for both personal and non-personal data and the simple noun "control" to describe the position of a controller. In contrast to the DGA, a person may qualify as a controller within the meaning of these Principles irrespective of whether the person has a right to determine the purposes and means of its processing. This difference can be explained by the fact that the DGA's subject matter is limited to facilitating data sharing. The DGA's terminology would not be suitable for the purposes of these Principles, as they have a much broader scope and also address the wrongfulness of data activities.

Given that the concept of "processor," which was originally developed by European law and has recently become widely used also in the United States and other parts of the world, these Principles have decided to adopt the term too. The main difference between a "controller" and a "processor" is that the latter follows the directions given by the first, i.e., the "controller" engages in processing, either by processing the data itself or by having "processors" process them on its behalf. While the controller determines the purposes and means of the processing, i.e., the why and how of the processing, practical aspects of implementation ("non-essential means") can be left to the processor. If the controller's instructions leave a margin of discretion, the processor may choose technical and organizational means that best serve the controller's interests. However, if the processor does not follow the instructions of the controller and determines its own purposes and means of the processing, the processor becomes a controller (Article 28(10) GDPR; European Data Protection Board (EDPB), Guidelines on the Concepts of Controller and Processor in the GDPR, 2020, p. 3 f).

d. "Co-generated data" and "derived data." The term "co-generated data" was coined by these Principles and has already been adopted by the European Commission in its European Data Strategy (COM(2020) 66 final, p. 10), the German Data Ethics Commission (Opinion of the German Data Ethics Commission, 2019, p. 133 ff.), and the Global Partnership on AI (GPAI) (see GPAI Working Group on Data Governance, A Framework Paper for GPAI's work on Data

Governance, 2020). The underlying idea that parties who have contributed to the generation of data should have some rights in the utilization of the data is also recognized in the Japanese Ministry of Economy, Trade and Industry's Guidelines (METI Guidelines, p. 45). While the term "data rights" is not defined or used in EU law, it is used in more recent legal literature to describe rights that do not clearly qualify as personality rights or property rights but lie somewhere in between (see Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds), The Evolution of EU Law, 3rd edn 2021; Yuming Lian, Data Rights Law 1.0: The Theoretical Basis, 2019, p. 98 ff). This understanding corresponds with the definition chosen by these Principles.

Different terms have been developed to describe data resulting from different forms of processing. For example, the terms "derived" data and "inferred" data are often used as synonyms for data that was created by drawing conclusions from provided datasets (see Organisation for Economic Co-operation and Development (OECD), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 31; METI, Contract Guidelines on Utilization of AI and Data – Data Section, 2018, p. 19; EDPB, Guidelines 8/2020 on the targeting of social media users, Version 1.0, 2 September 2020, p. 22; see also Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10). "Aggregated data" usually refers to the combination of initially separated data sets (Bertin Martens et al., Business-to-Business data sharing: An economic and legal analysis – JRC Digital Economy Working Paper 2020-05, 2020, p. 5, 12). Due to lack of a clear terminology in that regard, and the difficulties of drawing a distinct line between derived, aggregated, and structured data, these Principles have—as with the notion of processing—opted for a more generic definition to cover any data resulting from any kind of processing or other data activities.

e. "Data contracts," "data rights," and "data activities." The definitions of the terms "data contract" and "data activities" are specific to these Principles. EU legislation does not define them, and no definite meanings have been attached to the terms in legal literature. However, they seemed to be useful for the purpose of, in particular, Parts II and IV of these Principles.

f. "Supply," "supplier," and "recipient." Regarding the terms "supply" and "supplier," reference can, in particular, be made to Article 2(10) in the Proposal of the Digital Content and Services Directive (COM(2015) 634 final), which defines "supply" as providing access to digital content or making digital content available. However, it needs to be noted that the definition was dropped in the final text of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770). Other documents use the term "data provider" to refer to the party who provides data under a data provision type contract (METI, 'Contract Guidelines on Utilization of AI and Data – Data Section', 2018, p. 19).

Article 4(9) of the GDPR, defines "recipient" as a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. These Principles use the term in a somewhat narrower sense, close to the meaning adopted by the METI Guidelines, which understand data recipient to be "the party who receives data under a data provision type contract" (METI, 'Contract Guidelines on Utilization of AI and Data – Data Section', 2018, p. 19). This definition is similar to the one in the Data Act proposal, which defines the "data recipient" as the "legal or natural person [. . .] to whom the data holder makes data

available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law."

g. "Transfer," "porting," and "erasure." The term "transfer" of data is used in Chapter V GDPR and was also used in the EU-U.S. Privacy Shield (Commission Implementing Decision (EU) 2016/1250), which was recently discarded as void by the Court of Justice of the European Union (CJEU) in its latest judgment on the matter (Case C-311/18 ECLI:EU:C:2020:559 – *Schrems II*).

As to "porting," there is no official European definition even though the term is used in the heading of Article 6 of the Free Flow of Data Regulation (Regulation (EU) 2018/1807). In Article 20 of the GDPR, the right to "data portability" is implicitly defined as the right of a data subject to receive personal data which the data subject has provided to a controller, in a structured, commonly used, and machine-readable format, and to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. A similar description is provided by Article 16(4) of the DCSD. "Porting" can mean transfer both to the person entitled to porting and to a third party. The Data Act proposal sets out a "right to share data with third parties" in Article 5, which entitles users to request from data holders that the data generated by the use of a product or related service is made available to a third party. The word "porting" is, however, not used in the Data Act proposal.

"Erasure" of data is mentioned, but not defined, by Article 17 of the GDPR. Thus, it is still under discussion whether data is erased under the GDPR only when it is absolutely impossible to retrieve the data or when retrieving data would require unreasonable effort (see Sven Hunzinger, Das Löschen im Datenschutzrecht, 2018, p. 55 ff). These Principles follow the latter approach by setting out that "erasure of data means taking steps to ensure, as far as is reasonably possible, that the data is permanently inaccessible or otherwise unreadable."

h. "Notice." The definition of "notice" is inspired by the requirement that a person "knew or ought, under the circumstance, to have known" a certain fact, which is a central requirement in various civil law doctrines (see, for example, Article II. – 7:207 Draft Common Frame of Reference (DCFR); Article 4:109 Principles of European Contract Law (PECL) on excessive benefit or unfair advantage; Article VIII. – 3:101 f. DCFR on good-faith acquisition of ownership; Article VIII. – 3:101 f. DCFR on reversal of enrichment). At the European level, one of the most conspicuous examples is probably Article 4(4) and (5) of the Trade Secrets Directive (Directive (EU) 2016/943).

Principle 4. Remedies

(1) Remedies with respect to data contracts and data rights, including with respect to any protection of third parties in the context of data activities, should generally be determined by the applicable law.

(2) When these Principles or applicable law mandate the return or surrender of data by a party (the defendant) to another party (the claimant), the defendant should be able to satisfy the obligation to return or surrender the data by, instead, erasing all of the defendant's

copies of the data. If the claimant does not have a copy of the data, the defendant must put the claimant in control of the data before erasing it.

Comment:

a. Remedies. These Principles do not generally address remedial matters, leaving that to applicable law. Often, applicable law assesses money damages or monetary restitution as the remedy. However, there are also a number of cases in which the applicable law may require specific performance, and some jurisdictions, in particular in continental Europe, may have a general tendency toward preferring specific performance over money damages.

b. Return as part of a remedy. Sometimes, applicable rules or principles require the return of an item, including data, that was delivered to a party—for example, when data has been supplied by mistake, or when a contract was avoided or canceled after data was already supplied. Return is an elusive concept for data of which there can be many copies. Hence, paragraph (2) reflects the unique character of data and adjusts the duty to return accordingly. It provides that data may be "returned" by erasing all copies of the data that the recipient may still have under its control. If the supplier does not have a copy, e.g., because the parties had agreed that the recipient would have exclusive control and the supplier had undertaken to erase all of its copies, the recipient must put the supplier in control of a copy again before erasing its copies.

Illustration:

21. Employees of a department of company S transmit industrial data to company R in the erroneous belief that a contract between S and R about the supply of the data has been concluded. (Actually, negotiations failed at the last moment.) If applicable law would otherwise require R to return the mistakenly supplied data, R may instead erase all copies of the data of which it has control. If S's employees erased all of S's copies of the data—perhaps because that was a term of the (failed) contract—R must put S in control of the data before erasing it.

There may be situations in which, in light of the circumstances mandating the return, and the legitimate interests of the claimant as well as any protected third party, it may be more reasonable to make an allowance in money to be paid to the claimant instead of return by erasure. Determining whether this is the case requires a careful analysis of the individual circumstances,

which is why these Principles do not take a general stance on this matter. For a specific situation in which these Principles do provide guidance in this regard, see, however, Principle 36(2).

REPORTERS' NOTES

United States:

Under U.S. contract law, remedies for breach of contract "serve to protect one or more of the following interests of a promisee":

> (a) his "expectation interest," which is his interest in having the benefit of his bargain by being put in as good a position as he would have been in had the contract been performed,
>
> (b) his "reliance interest," which is his interest in being reimbursed for loss caused by reliance on the contract by being put in as good a position as he would have been in had the contract not been made, or
>
> (c) his "restitution interest," which is his interest in having restored to him any benefit that he has conferred on the other party.

Restatement of the Law Second, Contracts § 344 (AM. L. INST. 1981).

Also:

> The judicial remedies available for the protection of the interests stated in § 344 include a judgment or order
>
> (a) awarding a sum of money due under the contract or as damages,
>
> (b) requiring specific performance of a contract or enjoining its non-performance,
>
> (c) requiring restoration of a specific thing to prevent unjust enrichment,
>
> (d) awarding a sum of money to prevent unjust enrichment,
>
> (e) declaring the rights of the parties, and
>
> (f) enforcing an arbitration award.

Id. § 345.

The Uniform Commercial Code (UCC) gives primacy to protection of the expectation interest. See UCC § 1-305(a) (2021-2022 ed.) ("The remedies provided by [the Uniform Commercial Code] must be liberally administered to the end that the aggrieved party may be put in as good a position as if the other party had fully performed but neither consequential or special damages nor penal damages may be had except as specifically provided in [the Uniform Commercial Code] or by other rule of law").

As for circumstances in which return of data may be an appropriate remedy, see generally Restatement of the Law Third, Restitution and Unjust Enrichment § 54 (AM. L. INST. 2011).

Europe:

a. Remedies. With respect to data contracts, the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) provides for harmonized remedies for the failure to supply digital content or services, and the lack of conformity of digital content or services, in business-to-consumer (B2C) contracts. If the trader has failed to supply the digital content or digital service,

the consumer shall call upon the trader to do so. If the trader then fails to supply the digital content or digital service without undue delay, or within an additional period of time, the consumer shall be entitled to terminate the contract (Article 13(1) DCSD). In the case of a lack of conformity of the digital content or services with the contract, the consumer shall be entitled to have the digital content or digital service brought into conformity, to receive a proportionate reduction in the price, or to terminate the contract (Article 14(1) DCSD). The consumer is primarily entitled to have the digital content or digital service be brought into conformity, and only at a secondary stage to receive a proportionate price reduction, or to terminate the contract.

With the DCSD and the Consumer Rights Directive (CRD) (Directive 2011/83/EU as recently adapted by Directive (EU) 2019/2161) rules have been introduced also for the unwinding of a contract for the supply of digital content or services after the consumer's termination, in particular in cases in which there is a lack of conformity with the contract. There are also a host of consumer-specific remedies in other sectors, such as for the sale of goods or for package holidays.

Outside the realm of B2C relationships, remedies for breach of contract are mostly dealt with under non-harmonized national law, which varies to a great extent. However, generally speaking, the continental European legal systems favor specific performance as the primary remedy, and only if this fails or is inappropriate for some reason, other remedies, such as price reduction, rescission or termination, or damages, would be provided. The common-law jurisdictions, on the other hand, take a more favorable position toward damages as the remedy that is the most appropriate in many scenarios. The various general Principles that have been formulated by academics at the European level, such as Chapter 9 of the Principles of European Contract Law (PECL) or Book III, Chapter 3, of the Draft Common Frame of Reference (DCFR), tend to strike a balance between the common-law position and the continental position.

Remedies for the breach of third-party rights are not harmonized to the same extent as contractual remedies. However, when a European act provides for non-contractual rights and obligations, the same act sometimes provides remedies for the breach of those rights and obligations. One example is the Enforcement Directive (Directive 2004/48/EC), which enables the holder of an intellectual property right to request corrective measures (Article 11), such as the recall or destruction of the goods that infringe the intellectual property right, as well as to claim damages and legal costs (Articles 14 f). Another example is the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which entitles the data subject to an effective judicial remedy against a controller or processor (Article 79 GDPR).

Most EU instruments, however, leave the remedies for the breach of a non-contractual obligation to the Member States. This is the case in the Database Directive (Directive 96/9/EC), which sets out that the "Member States shall provide appropriate remedies in respect of infringements of the rights provided for in this Directive."

b. Return as part of a remedy. Paragraph (2) of this Principle is inspired by the DCSD, the CRD and the Trade Secrets Directive (Directive (EU) 2016/943).

According to the DCSD, the consumer shall, upon termination and at the request of the trader, return a tangible medium when digital content was supplied on such a medium. In any case, the consumer shall refrain from using the digital content or digital service and from making it available to third parties (Article 17(1) DCSD). The trader may prevent any further use of the

digital content or digital service by the consumer, in particular by making the digital content or digital service inaccessible to the consumer or disabling the user account of the consumer (Article 16(5) DCSD; Article 13(8) CRD). Article 16 of the DCSD and Article 13(5) and (6) of the CRD obligate the trader to make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader, and to refrain from using the content.

Under Article 12(1) of the Trade Secrets Directive the infringer must stop the use of the trade secret and destroy all or part of any document, object, material, substance, or electronic file containing or embodying the trade secret or, when appropriate, deliver up to the applicant all or part of those documents, objects, materials, substances, or electronic files.

PART II
DATA CONTRACTS

CHAPTER A
RULES AND PRINCIPLES GOVERNING DATA CONTRACTS

Principle 5. Application of these Principles to Data Contracts

Data contracts under Part II should be governed, in the following order of priority, by:

(a) rules of law that cannot be derogated from by agreement;

(b) the agreement of the parties;

(c) any rules of law other than those referred to in subparagraph (a) that have been developed for application to data transactions of the relevant kind;

(d) the terms included in the contracts by operation of Principles 7 to 15;

(e) application by analogy of default rules and principles of law that are not directly applicable to data transactions of the relevant kind but that would govern analogous transactions; and

(f) general principles of law.

Comment:

a. Hierarchy of sources. This Principle provides a general hierarchy for determining the rules governing data contracts.

At the top of that hierarchy are mandatory rules of applicable law that cannot be varied by agreement. Such mandatory rules differ from jurisdiction to jurisdiction. Examples of such rules include doctrines of unconscionability or unfairness control, obligations of good faith and fair dealing that cannot be disclaimed, prohibitions on excessively large liquidated damages, and also certain mandatory requirements to be included in contracts between controllers and processors under the law of some jurisdictions.

Next in priority is the agreement of the parties. This is because principles of party autonomy present in most legal systems give parties to a contract wide leeway to determine the terms of their relationship. Of course, what counts as the "agreement of the parties" is partly an issue of fact and partly the result of applying the rules of the applicable legal system as to what constitutes an agreement and how binding agreements are formed, as well as rules that determine which

communications are to be treated as part of an agreement when varying communications—oral as well as written or electronic—have been exchanged.

Many data transactions are the subject of extensive negotiations and careful contract drafting, while others are entered into with significantly less individualized attention. Disputes about the rights and obligations of parties do not typically arise when the subject of the dispute is covered by express agreement of the parties. Rather, they arise more often with respect to issues not covered in that agreement. All agreements are inevitably incomplete, with the result that, in the event of dispute, law is called upon to fill the gaps. In some cases, the issue may be one that was simply not addressed by the parties; in other cases, the parties may have thought the resolution was implicit in their agreement. For issues of this sort that arise with some frequency, contract law often deals with this phenomenon by providing for terms that are "automatically" included in a contract unless derogated from by agreement of the parties. Such terms are usually referred to as "default" terms or "implied" terms. Subparagraphs (c) to (e) of this Principle set out, in order of priority, how law fills the gaps in parties' agreements in determining their rights and obligations.

First, subparagraph (c) defers to contract law rules of the relevant jurisdiction insofar as they have been developed for application to data transactions of the relevant kind. Some states may have such data-specific rules, while others may not. Next, subparagraph (d) refers to Principles 7 through 15, which develop recommended default rules for nine types of data transactions. Finally, subparagraph (e) provides for the application of default rules and principles that apply to analogous transactions. As it is often difficult to identify contract law principles to govern a contract by analogy, Principles 7 through 15 also supply a list of factors a court should consider when deciding whether to adopt rules by analogy in the context of the particular types of data transactions addressed in those Principles. In applying rules by analogy under subparagraph (e), terms in those rules should be adjusted to the context of data transactions. So, for example, references to ownership must sometimes be replaced by references to control of the data, references to use or the like must sometimes be replaced by references to access to data, and references to delivery or the like must sometimes be replaced by references to the provision of control or access. For matters not addressed in subparagraphs (c) to (e), subparagraph (f) of this Principle ultimately defers to general principles of law to fill remaining gaps. These general principles will, in the first place, be general principles of contract law, but could equally be general principles of other bodies of law.

REPORTERS' NOTES

United States:

Freedom of contract plays a large role in the U.S. law of contracts. See, e.g., Restatement of the Law Second, Contracts, Introductory Note to Chapter 8 (AM. L. INST. 1981) ("In general, parties may contract as they wish, and courts will enforce their agreements without passing on their substance. . . . The principle of freedom of contract is itself rooted in the notion that it is in the public interest to recognize that individuals have broad powers to order their own affairs by making legally enforceable promises").

For transactional rules of law that cannot be derogated from by agreement, see generally, e.g., Uniform Commercial Code (UCC) § 1-302 (2021-2022 ed.). For data-specific rules of law that cannot be derogated from by agreement, see, e.g., California Consumer Privacy Act § 1798.192 ("Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."). Consumer protection law provides many additional examples of transactional rules that cannot be derogated from by agreement.

In addition to providing for specific rules that cannot be derogated from by agreement, U.S. contract law places limits on freedom of contract by limiting enforcement in the context of oppressive contracts and contracts the enforcement of which would be inconsistent with public policy. As to unconscionability, see UCC §§ 2-302 and 2A-108 and Restatement of the Law Second, Contracts § 208 (AM. L. INST. 1981) ("If a contract or term thereof is unconscionable at the time the contract is made a court may refuse to enforce the contract, or may enforce the remainder of the contract without the unconscionable term, or may so limit the application of any unconscionable term as to avoid any unconscionable result.") See also Model Computer Information Transactions Act (MCITA) § 111 (last revised or amended 2002). As to public policy, see, e.g., Restatement of the Law Second, Contracts §§ 178 et seq. (AM. L. INST. 1981). For default rules specifically relating to data transactions, see, e.g., Principles of the Law, Software Contracts (AM. L. INST. 2010). For the rationale for default rules in such transactions, see MCITA, Prefatory Note:

> Both MCITA and UCC Article 2 are based upon the principle of freedom of contract: with limited exceptions, the terms and effect of a contract can be varied by agreement. Most provisions of both statutes are default rules, applicable only if the parties do not specify some other rule. Although one could try to fashion a contract code that regulates comprehensively rather than permitting such flexibility, it is hard to imagine such an approach being compatible with a vibrant market economy. Even if one succeeded in making the regulations stick, the effect would be to hinder rather than facilitate commerce. On the other hand, as noted, without certain default rules, contracting and thus legal rights remain unclear.

For one critique of applying rules from other areas of law to data transactions by analogy, see Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863 (2019). For application by analogy of principles governing

other types of transactions, see generally Daniel E. Murray, *Under the Spreading Analogy of Article 2 of the Uniform Commercial Code*, 39 FORDHAM L. REV. 447 (1971), available at: http://ir.lawnet.fordham.edu/flr/vol39/iss3/3. See also Stacy-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 117 (2017); Peter A. Alces & Aaron S. Book, *When Y2K Causes "Economic Loss" to "Other Property*," 84 MINN. L. REV. 1 (1999). As to general rules of contract law, see Restatement of the Law Second, Contracts (AM. L. INST. 1981).

For discussions about optimal default rules in contracts, see, e.g., Oren Bar-Gill & Omri Ben-Shahar, *Optimal Defaults in Consumer Markets*, 45 J. LEGAL STUD. S137 (2016).

Europe:

Freedom of contract is a fundamental principle of European Law, which is only restricted by mandatory law, i.e., rules of law that cannot be derogated from by agreement, cf. Articles 1:103 Principles of European Contract Law (PECL), Article II.–1:102 Draft Common Frame of Reference (DCFR), and Article 0:101 *Principes du droit européen du contrat*.

At the European level, most of the rules on business-to-consumer (B2C) contracts are of mandatory nature (see, for example, Article 25 Consumer Rights Directive, Directive 2011/83/EU; Article 22 Digital Content and Services Directive (DCSD), Directive (EU) 2019/770; Article 21 SGD, Directive (EU) 2019/771), but allow agreements that are not detrimental to the consumer. In addition, unfairness control plays an important role with regard to contractual clauses that have not been individually negotiated due to the Unfair Contract Terms Directive (UCTD) (Council Directive 93/13/EEC). For business-to-business (B2B) contracts, the extent to which jurisdictions extend unfairness control to B2B relationships varies. There are some jurisdictions (e.g., German law) where unfairness control for B2B contracts is very similar to the situation in consumer law, and other jurisdictions (e.g., UK law) that are heavily opposed to any interference with B2B relationships. EU law has taken a very cautious approach on mandatory rules so far, but there is clearly a recent tendency toward unfair contract terms control also for B2B contracts. Examples can be found in the revised Late Payments Directive (see Article 7 Directive 2011/7/EU) or the Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain (Directive (EU) 2019/633). This trend is continuing with the Data Act proposal (COM(2022) 68 final), which provides for an unfairness test with regard to terms concerning data access and use that have been unilaterally imposed by an enterprise on micro-, small-, or medium-sized enterprises (Article 13). A term is considered unfair and not binding if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing. In addition to this general clause, the Data Act proposal contains a (black)list of terms that are considered unfair and a (grey)list of terms that are presumed unfair (Article 13(3) and (4)). The list includes terms that place certain limitations on usage rights in data to which the party has contributed or that were generated by a party during the period of the contract. The underlying notion of this unfairness control coincides with the concept of data rights with regard to co-generated data in Part III of these Principles.

It is in a similar vein that the Platform to Business Regulation (P2B) (Regulation (EU) 2019/1150) provides for transparency obligations the platforms have toward their business users.

According to its Article 9, platform providers must include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, that business users or consumers provide for the use of the platform services concerned or that are generated through the provision of those services. However, there are also tendencies toward self-regulation, e.g., in the Free Flow of Data Regulation (Regulation (EU) 2018/1807). According to its Article 6, the Commission shall encourage and facilitate the development of codes of conduct that address data portability in B2B relationships. It is to be expected that such codes of conduct, which are currently being developed (cf. COM(2018) 232 final p. 10 f., EU Code of conduct on agricultural data sharing by contractual agreement from April 2018), and which address also a number of issues besides portability rights, will establish standards whose effect in practice (e.g., for purposes of unfair contract terms control, or for gap-filling) may come close to the effect of default rules. While the Data Act proposal itself does not contain any default rules, Article 34 provides that the European Commission shall develop and recommend non-binding model contractual terms on data access and use.

At the national level, the effects of mandatory law on contractual agreements, such as nullification of a contract, are expressed separately, often in the same provision of the code that also addresses public policy. This applies to Section 879(1) of the Austrian Civil Code ("A contract that violates a legal prohibition or offends against common decency is void") or Article 1162 of the French Code Civil, which states that a "contract may not derogate from public policy either by its stipulations or by its purpose." Similarly, under the terms of Section 134 of the German Civil Code, a transaction is void if it violates a statutory prohibition.

While the Digital Content and Services Directive (DCSD) only applies to B2C relationships, its provisions are expected to greatly influence also the development of default rules for a range of data transactions (see, for example, Section 1(3) of the Austrian Implementation Act in which the update obligation was extended to B2B relationships). The definitions given for "digital content" (Article 2(1) DCSD: "data which are produced and supplied in digital form") and "digital service" (Article 2(2) DCSD: "a service that allows to create, process, store or access data in digital form or a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service"), it makes clear that the focus of the DCSD is not identical with the focus of these Principles. Arguably, the DCSD targets "functional data," and not transactions in which the "primary focus is on information" (see Principle 2(1)). Even though the focus of the Directive is on functional data, and the fact that there will only be exceptional cases in which data contracts within the meaning of these Principles are concluded in B2C relationships, it cannot be ignored that the broad notion of "digital content" in the DCSD (Article 2(1)) also covers data within the scope of these Principles. This means that, at least in B2C relationships, there already exist advanced rules on "data contracts," which, according to subparagraph (a) of this Principle, take priority over the Principles in Part II.

However, the DCSD does not cover all data contracts under Part II, and the focus of the Directive is also clearly on consumer protection, which is why it provides for very different obligations for the trader (supplier) of the digital content and the consumer (recipient). The most obvious overlap is with contracts for the transfer of data under Principle 7 and contracts for access to data under Principle 8. However, unlike these Principles, the DCSD does not contain different

rights and obligations depending on the mode of supply, but treats both contracts the same. The focus on the functional dimension of data also makes it hard to qualify contracts for the supply of digital content as contracts for the transfer of data or for access to data. While it is the trader under the DCSD that supplies the digital content to the consumer (as recipient), the trader can also be classified as the recipient when the consumer does not pay or undertakes to pay a price but provides or undertakes to provide personal data to the trader (see Article 3(1) DCSD). Such a contract would certainly qualify as a contract for the authorization to access under Principle 10.

The DCSD contains provisions on the mode of supply and implied warranties, including concerning a recipient's right to receive updates, which also inspired the duties set out for the supplier under Principles 7 and 8. However, the DCSD does not provide for detailed rules on control and use of the supplied data by the consumer that are comparable with those set out by these Principles, but only contains obligations of the consumer in the event of termination of the contract, when the recipient shall refrain from using the digital content or digital service and from making it available to third parties (Article 17 DCSD).

In continental Europe, gaps are primarily filled by non-mandatory rules (Austrian and German: *abdingbare* or *dispositive Rechtsvorschriften*, Dutch: *aanvullende rechtsregels* or *regelend recht*, French: *règles de droit supplétives*, Italian: *norme dispositive*, Spanish: *normas dispositivas*), which are found in civil codes, specific statutes, and in case law (cf. Hein Kötz, European Contract law, 2nd Edition, 2017, p. 102 ff.) The Principles in Part II could be an inspiration for the development of such non-mandatory rules on data contracts that apply in case such contracts are incomplete.

The application of rules *per analogiam* is one of the central methodological tools at the national and European levels (see Jörg Neuner, Judicial Development of Law, in Karl Riesenhuber (ed.), European Legal Methodology, 2017, p. 291 ff). The analogous application of rules that have been developed for similar transactions has already played a major role with regard to software contracts (i.e., what these Principles call "functional data"). Due to the narrow notion of "good" in some European jurisdictions, which does not cover non-rivalrous goods, contracts about software would not have classified as a sale, a lease, or a service contract because the object of the transaction does not qualify as a "good." However, most European jurisdictions applied their rules per analogy (see the Reporters' Notes to Principle 7). Similar problems will also arise when it comes to data contracts under Part II of these Principles, but the main difference is that these Principles provide for default rules specifically tailored to data contracts, which take priority over the rules mentioned in subparagraph (e) of this Principle.

Finally, data contracts are governed by the general rules and principles of contract law. Such general rules and principles exist at the national level, but several attempts have also been made to formulate them at the European level, such as by the Principles of European Contract Law (PECL), the Draft Common Frame of Reference (DCFR), the Principles of the Existing EC Contract Law (Acquis Principles), the *Principes du droit européen du contrat*, or the Common Core of European Private Law Project of the Trento Group. They can further be found on a more international level in the UNIDROIT Principles of International Commercial Contracts (UPICC).

Principle 6. Interpretation and Application of Contract Law

In interpreting and applying rules and principles of contract law, the following factors, among others, should be considered:

(a) the fact that data is a combination of (i) physical manifestations on a medium or in a state of being transmitted, and (ii) information recorded;

(b) the nature of data as a resource of which there may be multiple copies and which can be used in parallel by various parties for a multitude of different purposes;

(c) the fact that data is usually derived from other data, and that the original data set and a multitude of derived data sets that resemble the original data set to a greater or lesser extent may coexist;

(d) the fact that, while the physical location of data storage may change quickly and easily, data is normally utilized by way of remote access, and the physical location of data storage is typically of little importance; and

(e) the high significance of cumulative effects and effects of scale.

Comment:

a. General observations. The subject of data contracts is different, in many ways, from the subject of many other contracts. Because of those differences between the subject of data contracts and that of many other contracts, application of general principles of contract law, often designed for those other contexts, should be sensitive to those differences. In some cases, this will involve interpretation of general principles in a manner that is consistent with the context in which they are to be applied. In other cases, these differences will guide and constrain analogies to principles of law that govern different subjects.

This Principle comes into play at several of the levels within the hierarchy of rules established in Principle 5. When there are mandatory rules of law, i.e., rules of law that cannot be derogated from by agreement, within the meaning of Principle 5(a), those mandatory rules may have been drafted with traditional transactions about traditional resources (such as goods or rights) in mind. When they need to be applied to a data contract, the specificities of data must be taken into account. Even more, when default rules and principles of law that are not directly applicable to data transactions of the relevant kind are applied by analogy within the meaning of Principle 5(e), those rules and principles normally must be adapted to fit in the data context. The same holds true for general principles of law, including contract law, within the meaning of Principle 5(f).

b. Factors to be considered. This Principle lists some factors that should be considered when applying contract law that was not drafted with data transactions in mind. An important special feature of data is the fact that data is a combination of binary impulses that may be physically manifest on a medium or be transmitted, and the information recorded in those binary impulses. This means that, e.g., the act of supplying data is closer to "delivering" but certainly has a "doing" element, and, accordingly, a contract to supply data is somewhat in between a sales contract and a service contract.

Illustration:

22. If A sells a machine to B, that transaction can be described as being about delivering something, and if A promises to provide legal advice to B, that is clearly a service. However, if A shares data with B, that is somewhat in between delivering something to B (i.e., the binary impulses, by way of transmission) and doing something for B (i.e., triggering a change in the state of B's storage device), which makes it difficult, for instance, to seek proper analogies.

Another important feature that makes data different from almost all other resources is its non-rivalrous nature, i.e., the fact that there may be multiple copies of one and the same set of data, which can be used in parallel by various parties for a multitude of different purposes.

Illustration:

23. If A sells a machine to B, A will no longer have the machine, but if A sells data to B, both A and B can have and use the data, and the multiplication of the data does not in any way reduce its practical utility (without prejudice to the fact that the market value of data may decrease rapidly with increasing numbers of persons having the data). This may affect the way in which a court would apply rules and doctrines such as on the passing of risk, because if data is lost or destroyed while being transmitted from the supplier to the recipient, the supplier is able to transmit another copy at no or only negligible cost.

A similar feature of data is that data can be changed within fractions of a second, and that almost all data is derived from other data, with the changed or derived set of data often existing in parallel with all the previous versions, partly coinciding with previous versions, and partly not.

Illustration:

24. If A rents a cow to B, it is clear that, when the contract term comes to an end, B must return the cow, and, if the cow has meanwhile given birth to a calf, possibly the calf (depending on the applicable contract and property law). If A gives access to data to B for a particular access period, the law will not only have to mandate that B erase any copies of the data B may have retained (on which, see subparagraph (b) of this Principle as well as Principle 4(2)), but will also have to decide which data sets that have, in one way or another, been derived from A's data set, are included in the duty to return.

Another characteristic feature of data is the fact that, while the physical location of data storage may change within fractions of a second, the data is normally utilized by way of remote access, and the storage location is of little relevance.

Illustration:

25. If A sells a machine to B, contract law may provide for rules on the place of performance, e.g., the default rule might be that the place of performance is the place of establishment of seller A, but that it is the establishment of C if the machine is currently in the possession of C. However, if A supplies data to B, it may not necessarily make sense to identify the place of performance according to the same rules, in particular as, with cloud-based storage, the location of data may no longer play any meaningful role. Indeed, the concept of a "place" of performance may have little meaning in this context.

Finally, it is the unusually high significance of cumulative effects and effects of scale that make data different from other resources, in that the value of data depends largely on which other data they can be combined with, who has access to the data, and similar factors.

REPORTERS' NOTES

United States:

As to the non-rivalrous nature of data, see, e.g., Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data* (Sept. 2019), NBER Working Paper No. w26260, available at SSRN: https://ssrn.com/abstract=3454361 ("The starting point for our analysis is the observation that data is nonrival. That is, at a technological level, data is infinitely usable. Most goods in economics are rival: if a person consumes a kilogram of rice or an hour of an accountant's time, some resource with a positive opportunity cost is used up. In contrast, existing data can be used by any number of firms or people simultaneously, without being diminished. Consider a collection of

a million labeled images, the human genome, the U.S. Census, or the data generated by 10,000 cars driving 10,000 miles. Any number of firms, people, or machine learning algorithms can use this data simultaneously without reducing the amount of data available to anyone else").

Europe:

With regard to the characteristics of data, several sets of principles stress the need to give special attention to data, ensuring different treatment from goods or services, in particular in light of the non-rivalrous nature of the resource (see, for example, Organisation for Economic Co-operation and Development (OECD), Data-Driven Innovation - Big Data for Growth and Well-Being, 2015, p. 177 ff; OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 15 ff; European Commission, A European Data Strategy, COM(2020) 66 final; German Data Strategy (Datenstrategie der Bundesregierung), 2021, p. 15 ff; the French AI Strategy: Villani Report (2018), p. 20 ff).

Both the Principles of European Law and the Draft Common Frame of Reference (DCFR) state that their rules should also apply to contracts on data with "appropriate adaptations" (see, e.g., Article 1:105 Principles of European Law, Sales; Article IV.A. – 1:101(2)(d) DCFR). However, unlike this Principle, they do not provide a list of factors that should be considered when applying their rules and principles.

CHAPTER B
CONTRACTS FOR SUPPLY OR SHARING OF DATA

Principle 7. Contracts for the Transfer of Data

(1) A contract for the transfer of data is a transaction under which the supplier undertakes to put the recipient in control of particular data by transferring the data to a medium within the recipient's control, or by delivering to the recipient a medium on which the data is stored.

(2) Subject to agreement of the parties and to rules that take priority pursuant to Principle 5, the law should provide that the following terms are included in a contract for the transfer of data:

(a) With regard to the manner in which the supplier is to perform its undertaking described in paragraph (1), the data should be transferred in accordance with the recipient's directions, unless the mode of transfer indicated is unreasonable (e.g., in light of data security concerns), in which case the supplier should promptly notify the recipient of those concerns so that the recipient may substitute different directions for transfer.

(b) With regard to the characteristics of the data supplied, including with regard to nature, quantity, accuracy, currentness, integrity, granularity, and formats, as well as with regard to the inclusion of metadata, domain tables, and other specifications required for data utilization, and to frequency of supply and any updates:

(i) the supplied data must conform to any material descriptions or representations concerning the data made or adopted by the supplier, and to any samples or models provided;

(ii) if the supplier has notice of the recipient's particular purpose for obtaining the data, and that the recipient is relying on the supplier's skill or judgment in selecting the supplied data, the supplied data must be fit for the recipient's particular purpose; and

(iii) if the supplier is in the business of supplying data of the sort that is the subject of the contract or otherwise holds itself out as having expertise with

respect to data of that sort, the supplied data must be of a quality that would reasonably be expected in a transaction of the relevant kind.

(c) With regard to the control of, and other data activities with regard to, the supplied data:

(i) if the supplied data is protected by intellectual property law or a similar regime, the supplier must place the recipient in the position of having a legal right, effective against third parties, that is sufficient to result in the recipient's control of the data and the right to engage in such other data activities that the controller had notice that the recipient could reasonably expect to engage in; if putting the recipient in that position requires additional steps to be taken by the supplier, such as execution or recordation of a required document, the supplier must take those additional steps;

(ii) the supplier must place the recipient in a position, at the time the data is supplied, of being able rightfully to exercise control over the data and rightfully to engage in other data activities that the controller had notice that the recipient could reasonably expect to engage in; if, after the data has been supplied, the recipient's control of the data or other data activities become wrongful, this does not of itself give rise to a claim by the recipient against the supplier;

(iii) the supplier must cooperate, to the extent reasonably necessary, in actions that may be required to comply with legal requirements with respect to control of the data or other data activities that the controller had notice that the recipient could reasonably expect to engage in; in addition, the supplier must provide to the recipient information about any legal requirements with respect to any such data activities of which the supplier has notice and of which the recipient cannot be expected to be aware;

(iv) the recipient may utilize the data and any derived data, including by onward supply to others, for any lawful purpose and in any way that does not infringe the rights of the supplier or third parties, and that does not violate any obligations the supplier has vis-à-vis third parties, provided the recipient had notice of these obligations at the time the contract for the transfer of data was concluded;

(v) as between the parties, new intellectual property rights or similar rights created by the recipient with the use of the supplied data belong to the recipient; and

(vi) the supplier may retain a copy of the data and may continue using the data, including by supplying it to third parties.

(3) In determining which rules and principles should apply by way of analogy, as provided in Principle 5, to contracts for the transfer of data, consideration should be given in particular to:

(a) whether the contract provides for the recipient to be in control of the data for an unlimited period of time or for a limited period of time; and

(b) whether the contract is for a single supply of data, repeated supply, or continuous supply over a period of time.

Comment:

a. Scope. This Principle is the first of a series of Principles setting out default provisions for contracts concerning different types of data transactions. Under this Principle, A contract for the transfer of data is a transaction under which the supplier undertakes to supply particular data to a recipient, and, in doing so, to put the recipient in control of that data by transferring the data to a medium within the recipient's control or by delivering to the recipient a medium on which the data is stored. This type of contract may involve data of any kind, whether raw or derived, and whether or not protected by intellectual property law or a similar regime.

Illustration:

26. Supplier S operates an online shop and holds large amounts of customer data. S promises to recipient R to supply specified types of data (name, email address, goods bought, search requests made) regarding the shopping behavior of a specified number (20,000) of customers from specified regions (the United States and the European Union) that has accumulated over a specified period (24 months) and to transfer the data to a medium within R's control. The purpose of this deal is to enable R to engage in targeted advertising campaigns. This would be a contract for the transfer of data under this Principle.

A medium within the recipient's control may be, for example, the recipient's server. It may also be a cloud space to which the supplier gives the recipient the access credentials if the intention

is to allow the recipient to download the data from the cloud space onto a medium within the recipient's control, or if the cloud space is intended to remain within the recipient's control. The supplier may also deliver a storage device on which the data is stored.

b. Default terms as to the mode of supply. The parties to a contract for the transfer of data will typically agree how the data should be supplied to the recipient. If the contract is silent regarding the mode of supply of the data, paragraph (2)(a) provides relevant default terms. The default terms provide that the data is to be transferred in accordance with the recipient's directions. The recipient will typically choose to have the data transferred directly to a medium controlled by the recipient, or to have the data provided on a medium to which the recipient has or is given access (in accordance with Article 8(2)(a)(i)) and from which the recipient may port the data to a medium of the recipient's choice. However, the mode of transfer indicated by the recipient need not be accepted by the supplier if it is unreasonable, such as, for example, in case of data security concerns or when the transfer would be very costly.

Illustration:

27. Assume that, in the transaction in Illustration no. 26, recipient R directs supplier S to transfer the customer-related data to particular cloud space, but this cloud space is insecure, and thus not a reasonable mode of transfer. S is not obligated to transfer the data to the insecure cloud space. (This protects S from the possibility that S itself might be in breach of contractual and statutory duties if customer data is transferred to insecure storage space.)

When the mode of transfer is unreasonable, the supplier should promptly notify the recipient of those concerns so that the recipient may indicate a substitute.

c. Default terms as to the characteristics of the data. When the default terms relate to characteristics of the data that is the subject of the transaction, those terms are usually referred to as "warranties." Characteristics of data have many facets, some of the most important being: nature (including whether the data are personal data or nonpersonal data according to the applicable law), accurateness, currentness, integrity, granularity, and formats, as well as the inclusion of metadata, domain tables, and other specifications (such as ontologies) required for data utilization, and frequency of supply and any updates. The warranty terms set out in this Principle are analogous to warranty terms included as default terms in contracts for the sale of goods.

First, in some cases, even though the parties have not expressly stated in the contract the nature, quantity, and quality of the data, descriptions or representations concerning the data have been made or adopted by the supplier. When these descriptions or representations are part of the basis of the bargain, this Principle incorporates them into the contract. In those cases, it is appropriate for the supplier to be bound by those descriptions or representations as though they were expressly stated in the agreement of the parties. The same holds true if the supplier has provided the recipient with samples (such as a sample dataset) or models (such as the structure in which the information will be presented).

Illustrations:

28. Assume that, in the negotiation of the transaction in Illustration no. 26, supplier S states that the data sets have been updated within the last six months. Therefore, the contract includes a requirement that the data has, in fact, been updated within that period.

29. If, during the negotiation of the transaction in Illustration no. 26, supplier S provides recipient R with sample datasets of 100 typical customers, and in these datasets the names are complete and all of the fields, even the nonmandatory fields, are filled in, the contract includes a term that all datasets are as complete as the sample.

Second, if the supplier has notice of the recipient's particular purpose for obtaining the data and that the recipient is relying on the supplier's skill or judgment in selecting the supplied data, the supplied data must be fit for the recipient's particular purpose. While this is probably an exceptional situation in the data world, the selection and furnishing of data by the supplier in such circumstances could be seen as an implicit statement by the supplier that the data is fit for the recipient's purpose.

Illustration:

30. Assume that, in a situation of the kind described in Illustration no. 26, recipient R develops a new smart service that functions in conjunction with fitness bracelets from a defined range of manufacturers. R is interested in having access to customers who have bought such bracelets and might thus be interested in R's new service. R approaches supplier S, disclosing to S this purpose and indicating that it is relying on S in selecting appropriate data sets. S then declares that S has appropriate datasets for R, and the two enter

into a contract for the transfer of customer data. It is a term of the contract that the datasets supplied are fit for the purpose disclosed by R.

Third, according to paragraph (2)(b)(iii) a default term that the supplied data must be of a quality that would reasonably be expected in a transaction of the relevant kind becomes part of the contract if "the supplier is in the business of supplying data of the sort that is the subject of the contract or otherwise holds itself out as having expertise with respect to data of that sort." This condition to the presence of the default term is included because it is fair to require the supplier to stand behind the quality of data in situations in which the market has that expectation in light of the characteristics of the supplier. This is not a mandatory term, but the burden is on a supplier that does not want to have this responsibility for the quality of the data to negate the default term in the contract. This arrangement of responsibilities is similar to responsibilities for the quality of goods in many legal systems. One context is when the supplier is a business that collects large amounts of data as part of its business, such as a social network or a search engine provider. Another context occurs when a company that manufactures goods or provides services accumulates a substantial amount of data as part of its operations and goes into the separate business of selling that data.

Illustrations:

31. Shoe manufacturer S manufactures custom-made shoes for customers who supply foot measurements via a specially designed app. Accordingly, S has accumulated a large amount of data about foot sizes that is not available elsewhere. S concludes that there is a market for this sort of data among other shoe manufacturers, suppliers of orthopedic equipment, etc., and markets the foot-size data to companies in those industries. There is so much demand for this data that S makes significant profits every year supplying it. S is "in the business of supplying data of the sort that is the subject of the contract." Accordingly, the contracts for the transfer of data include the default term in paragraph (2)(b)(iii) of this Principle.

32. If, in a situation of the kind described in Illustration no. 26, supplier S has made trade in customer data part of its business and regularly engages in this to generate additional income, S can be expected to make sure the data is of the quality that is normal in transactions of the relevant kind. For example, when, in the relevant industry and under the relevant circumstances, the normal expectation would be that not more than about 15 percent of customer email addresses will fail at the point in time when the data is

transferred, the contract includes a term that the email addresses will conform to that expectation.

33. If, conversely, in a situation of the kind described in Illustration no. 26, supplier S simply runs an online shop and has just accumulated customer data for S's own purposes, but then is approached by R as to whether S might be prepared to sell the customer data (which S would initially not have planned, but is happy to do in order to generate additional income), the term that the email addresses will conform to the expectations in the relevant industry is not included in the contract.

d. Default terms with regard to control of, and other data activities with regard to, the supplied data. A third group of default terms concerns control and use of the supplied data by the recipient.

First, when the supplied data is protected under intellectual property law or a similar regime (such as EU investment protection for databases), the supply of that data would have little value if it did not include an appropriate legal right to use that data. The parties' intention is normally focused on the granting or assignment of a legal right that allows the grantee or assignee to have rightful control of that particular set of data, and that allows the recipient to engage in all data activities that the controller had notice that the recipient could reasonably expect to engage in, and that is effective vis-à-vis the rightholder and other third parties.

This Principle does not address whether and to what extent the supply of copyright-protected data should be characterized as a license contract or as a sale; this Principle applies under either characterization. The nature and extent of the right to be provided (e.g., whether it is a license for limited or for unlimited time, on how many servers the data may be stored and run, how many people may use the data at the same time), if not specified by the parties, should be broad enough to enable the use contemplated by the contract. If the right provided is insufficient for such use, the supplier's actions fall short of what this term requires and the supplier is liable for breach. Because some domestic intellectual property regimes require licenses to be memorialized in a writing or record, or require recordation of the writing or record (or a reference to it), paragraph (2)(c)(i) also addresses that situation.

Illustration:

34. The customer data that supplier S promises to transfer to recipient R in a situation of the kind described in Illustration no. 26 includes some photographic material

that customers have uploaded to share their experience with other customers, and that is protected by intellectual property law. Even if not expressly agreed, the contract includes a term according to which S must make sure R gets a license that allows R to do at least what R intends to do with the data when the contract is concluded, i.e., analyze the data for purposes of targeted advertising.

Even when data is not protected by intellectual property law, the usefulness of data to the recipient would be undermined if the recipient did not obtain rightful control over the data at the time it is supplied, or could not engage in other data activities that the controller had notice that the recipient could reasonably expect to engage in. Thus, paragraph (2)(c)(ii) states, as a default term, that the recipient must obtain such control. The supplier must therefore ensure that, for example, there are no legal barriers that would prevent the recipient from rightfully gaining control. Legal barriers could be barriers stemming, e.g., from data privacy/data protection law, from intellectual property law, or from a similar regime such as trade secrets law. The methods by which the supplier ensures the absence of legal barriers will depend on the individual circumstances. They could, e.g., include the seeking of valid consent or other forms of waiver of rights, or technical measures such as anonymization of data.

Illustration:

35. Assume that, in a situation of the kind described in Illustration no. 26, the agreement between supplier S and recipient R is silent as to whether S is responsible for ensuring that the customers, who are protected by a data privacy regime, have given all necessary consents to transfer of control of the data to R. S supplies the data, but 5,000 of the customers have not given their consent to the transfer of control of the data, with the result that, under the applicable data privacy regime, control of the data by R would be wrongful. S has violated its obligation under paragraph (2)(c)(i) to enable the recipient rightfully to exercise control over the data at the time it is supplied.

Unless the parties have agreed otherwise, subsequent facts rendering control or other data activities by the recipient wrongful (and possibly triggering a duty of the supplier to inform the recipient under Principle 32(2)), do not, as such, give rise to a claim by the recipient against the supplier.

Illustration:

36. Same facts as Illustration no. 35, except that, at the time of transfer, the customers all gave consent to the transfer of control of the data. After the data is supplied, however, 5,000 customers protected by a data privacy regime withdraw their consent to the transfer, with the result that, under the applicable data privacy regime, any future control or processing of these data by R would be wrongful. S has not violated its obligation under paragraph (2)(c)(i) to enable the recipient rightfully to exercise control over the data at the time it is supplied.

Third, there may be other legal requirements with respect to control and use of the data. Paragraph (2)(c)(iii) provides, as a default term, important obligations of the supplier with respect to such requirements. In particular, the supplier is obliged to provide the sort of support that can reasonably be expected in order to comply with legal requirements governing control and use of the data. In addition, although a recipient can be expected to be aware of the sort of legal requirements that apply to the control and use of data generally, paragraph (2)(c)(iii) includes a default term requiring the supplier to disclose any legal requirements that the recipient cannot be expected to be aware of, as far as the supplier has notice of them, and provide support to the recipient in complying with them.

Illustration:

37. In a situation of the kind described in Illustration no. 26, recipient R can be expected to be sufficiently aware of the general fact that both customers from the United States (e.g., residents of California) and customers from the European Union may be protected by data privacy regimes because this is a fact that should be known to anyone engaging in a data transaction. However, if it is not evident that some of the customer data qualifies as health data and is therefore subject to a much stricter regime, and R (who is not a very sophisticated recipient) cannot be expected to be aware of this stricter regime, S is under an obligation to inform R of this fact if S has notice.

Fourth, unless the parties have agreed to the contrary, it is appropriate to treat the contract as one that does not place any limits on how the recipient may utilize the data (including by passing it on), so a default rule to that effect is included. Thus, among the policy choices for default rules recommended by these Principles is that data supplied may be used by the recipient for any lawful

purpose that does not infringe the rights of the supplier or of third parties, including any obligations the supplier has vis-à-vis third parties provided the recipient had notice of these obligations. With regard to data that is not protected by intellectual property law, these Principles thus take a "sales" approach (i.e., freedom of the recipient is the default position, and limitations must be agreed upon), and not a "license" approach (which would mean that, as a default rule, the recipient may engage only in the data activities agreed upon).

Illustration:

38. As a default position, R would, in a situation of the kind described in Illustration no. 26, be allowed to utilize the customer data for any purpose R deems fit as long as this utilization does not infringe any rights of S or of third parties, including in particular the customers under an applicable data privacy regime. So, provided the data privacy law so allows, and there are no other specific restrictions on the use of the data (such as a duty of S of which R had notice when the contract was concluded), R would be free to change its mind and no longer (just) engage in targeted advertising, but instead (also) use the data for developing a new online reputation system.

In practice, however, it is quite common that parties supply data under a contract labeled a "license" even if they have really concluded a contract for the transfer of data, and specify in that "license" the conditions under which the supplied data may be used. If the data is not protected by intellectual property law, or no longer protected due to exhaustion (first sale doctrine), this is a contract covered by this Principle without regard to how the parties label it. If the parties make further agreements about the purposes for which the recipient may or may not process the data, about the number of people to whom the data may be disclosed, or about the duration of use by the recipient, they create, by virtue of freedom of contract, independent contractual obligations of the recipient to refrain from particular operations.

Illustration:

39. If the parties in a situation of the kind in Illustration no. 26 so wish, they may describe, in some detail, the types of data use recipient R may or may not engage in. In particular, they may agree that R must not compete with S on particular markets, or pass the data on to third parties. R is bound by this contractual restriction on data utilization.

In this context, it is important to highlight the connection between Principles 7 through 15 and Principles 32 through 34 inasmuch as the latter deal with the supplier's obligation to pass on certain restrictions and obligations to the recipient and to alert the recipient, (e.g., if subsequent events occur that are relevant for the recipient's legal position). In particular, Principle 32(1) obliges the supplier to impose particular contractual duties and restrictions on the recipient to the extent that these duties and restrictions must be complied with for the benefit of a protected party within the meaning of Part IV, Chapter A.

Fifth, the question of allocation of intellectual property rights created with supplied data is something parties to a transaction should normally agree on in advance, inasmuch as that allocation may have important economic effects. Under this Principle, there is a default term that these new intellectual property rights belong to the recipient. As with all default terms, this is subject to mandatory legal rules that cannot be derogated from by contract, and to agreement between the parties to the transaction. For example, applicable law might provide that new intellectual property rights are vested in a third party such as in an employee of the recipient.

Illustration:

40. Assume that in a situation of the kind described in Illustration no. 26, R would indeed use the data for developing a new online reputation system, which in itself would be protected by copyright. As a default position, S would not hold any rights in that system, and all intellectual property rights would be vested in R. This is, however, just as between the parties, so if the law provides that, really, the intellectual property rights should be vested in independent coder C, this is to be respected.

Sixth and finally, a contract for the transfer of data is not usually intended to deprive the supplier of the continuing right to use that data. Accordingly, paragraph (2)(c)(vi) provides a default rule to the effect that the supplier may retain a copy of the data and may continue using it, including by supplying it to third parties, i.e., any utilization rights of the recipient are normally nonexclusive.

Illustration:

41. In a situation of the kind described in Illustration no. 26, no one would expect supplier S to delete all of its customer data after having transferred them to recipient R. But there may be scenarios in which this is less self-evident, e.g., when the data relate to a type

of goods S wishes to stop offering on the market, while R wants to invest in selling precisely this type of goods. Still, in the absence of an agreement to the contrary, S would not be required to delete the data after the transfer.

e. Application of other law by analogy. Principle 5 provides that default rules and principles that are not directly applicable to the transaction at hand but that would govern a type of transaction akin to the transaction at hand may be applied to that transaction by analogy.

Since a contract for the transfer of data under which the recipient may use the data for an unlimited period of time will very often have many important characteristics of a sale, inasmuch as unlimited use transfers the economic value of the data to the recipient, the closest analogy may often be to the law of sale of goods, unless the relevant jurisdiction provides for specific rules on the supply of digital content. If, however, the terms of the contract provide that the recipient may use the data only for a limited period of time (whether or not enforced by the data being self-destructing and readable only for a limited period of time), the more appropriate analogy may sometimes be the law of lease contracts, or similar bodies of the law. Also, different sets of legal rules may apply depending on whether the contract is for a one-time exchange or for repeated or continuous supply.

The list in paragraph (3) of criteria to take into account when deciding which rules and principles to apply by analogy is not exhaustive. Other criteria that may be useful, depending on the circumstances, include the nature of the data and of any third-party rights in the data, and whether the supplier also promises, under the same contract, to customize the data sets that are to be supplied, which may recommend an analogy to the law of services contracts.

REPORTERS' NOTES

United States:

The terms included in a contract for the transfer of data under paragraph (1) can be analogized to the delivery terms in Uniform Commercial Code (UCC) § 2-503 et seq. (2021-2022 ed.). See also Model Computer Information Transactions Act (MCITA) § 606 (last revised or amended 2002). (In the 1990s, The American Law Institute and the Uniform Law Commission [the co-sponsors of the UCC] engaged in an effort to draft a uniform law that would govern many information transactions directly, with rules tailored specifically for that context. It was intended that the law would become a new Article of the UCC to be known as "Article 2B – Software Contracts and Licenses of Information." The effort foundered however, with the ALI withdrawing from the project in 1999. The Uniform Law Commission continued the project separately, promulgating it in revised form as the Uniform Computer Information Transactions Act, but efforts

at enactment have been unsuccessful, with two enactments in 2000 and none since. The product has since been renamed as the Model Computer Information Transactions Act.) The terms that are included in a contract for the transfer of data under paragraph (2) would typically be referred to under U.S. contract law as "implied terms."

The terms related to the characteristics of the data in paragraph (2)(a) are parallel to implied warranties under UCC Article 2 in the context of the sale of goods and under UCC Article 2A in the context of the lease of goods:

1. Descriptions or representations concerning the data that have been made or adopted by the supplier and have become part of the basis of the bargain would, if the subject of the contract were goods, be considered express warranties. See UCC §§ 2-313, 2A-210. See also MCITA § 402; Principles of the Law, Software Contracts § 3.02 (AM. L. INST. 2010).

2. When the seller or lessor of goods is a "merchant," the contract of sale or lease contains an implied warranty that the goods are "merchantable." To be merchantable, goods must satisfy several criteria including, most important for this context, that the goods would pass without objection in the trade and be fit for the ordinary purposes for which such goods are used. See UCC §§ 2-104, 2-314 and 2A-212. See also MCITA § 403; Principles of the Law, Software Contracts § 3.03 (AM. L. INST. 2010).

3. When a seller or lessor of goods has reason to know the particular purpose of the buyer or lessee and that the buyer or lessee is relying on the skill or judgment of the seller or lessor to select or furnish suitable goods, there is an implied warranty that the goods are fit for that purpose. See UCC §§ 2-315 and 2A-213. See also MCITA § 405(a); Principles of the Law, Software Contracts § 3.04 (AM. L. INST. 2010).

4. When goods are sold or leased, there is a warranty of title and against infringement implied in the contract. See UCC §§ 2-312 and 2A-211. See also MCITA § 401; Principles of the Law, Software Contracts § 3.01(AM. L. INST. 2010).

In addition to the MCITA, reference should be made to the Principles of the Law, Software Contracts (AM. L. INST. 2010), which address many of the same issues addressed in the MCITA, albeit not always reaching the same conclusion.

Courts have, on occasion, applied UCC Article 2 by analogy to transactions outside its formal scope, such as data and software contracts. See, e.g., Arbitron, Inc. v. Tralyn Broad., Inc., 400 F.3d 130, 138 & n.2 (2d Cir. 2005); i.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002). See generally Daniel E. Murray, *Under the Spreading Analogy of Article 2 of the Uniform Commercial Code*, 39 FORD. L. REV. 447 (1971).

Europe:

a. Scope. "Contracts for the supply of data" do not fall under any of the established contract types in continental European legal systems. However, EU law has a clear tendency to treat the supply of digital content like sales contracts. In its decision *UsedSoft* (Case C–128/11 UsedSoft ECLI:EU:C:2012:407), the Court of Justice of the European Union (CJEU) clarified that the supply of a computer program for an unlimited time against remuneration is to be considered a "sale" within the meaning of the Software Directive (Directive 2009/24/EC) and thus exhausts the copyright holder's distribution right for that copy. Regarding remedies for lack of conformity of

supplied digital content and services, the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) has introduced a uniform, sales-like regime.

Specific provisions for the transfer of data, however, do exist with regard to personal data. The European Commission has adopted so-called Standard Contractual Clauses (SCC) for the transfer of personal data to controllers and processors established in third countries (Commission Implementing Decision (EU) 2021/914). When an exporting controller and an importing controller or processor include the SCC in their contract, the transfer of the data outside the European Union is considered to be in accordance with EU data protection legislation, but a recent judgment of the CJEU (C-311/18 ECLI:EU:C:2020:559 – *Schrems II*) may mean that further steps are often required. While SCC are not contract law that governs the parties' contractual relationship without any agreement to that end, they provide important indications as to what the European legislator considers to be a reasonable and fair contractual arrangement.

b. Default terms as to the mode of supply. Given that there are not many examples in terms of specific rules on the supply of data in European legal systems, the main source for paragraph (2)(a) of this Principle is Article 5(2) of the DCSD. It provides that the trader shall have complied with the obligation to supply digital content or services when (a) the digital content or any means suitable for accessing or downloading the digital content is made available or accessible to the consumer, or to a physical or virtual facility chosen by the consumer for that purpose; or (b) the digital service is made accessible to the consumer or to a physical or virtual facility chosen by the consumer for that purpose. The fact that that provision does not include a reservation as to data security can easily be explained by the types of scenarios that the DCSD has been designed to address, i.e., mass contracts with consumers, in which the trader fully controls the mode of supply.

c. Default terms as to the characteristics of the data. The warranties laid down in paragraph (2)(b) of this Principle mirror to some extent the DCSD's conformity requirements for digital content and services. Traditionally, European legal systems differentiate between a subjective conformity test and an objective conformity test. According to Article 7 of the DCSD, subjective requirements for conformity are that the digital content or service (a) is of the description, quantity, and quality, and possess the functionality, compatibility, interoperability, and other features, as required by the contract; (b) is fit for any particular purpose for which the consumer requires it and which the consumer made known to the trader at the latest at the time of the conclusion of the contract, and in respect of which the trader has given acceptance; (c) is supplied with all accessories, instructions, including on installation, and customer assistance as required by the contract; and (d) is updated as stipulated by the contract. The objective requirements for conformity listed in Article 8 of the DCSD include that the digital content or service (a) is fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, when applicable, any existing law, technical standards, or sector-specific industry codes of conduct; (b) is of the quantity and possesses the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity, and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect, given the nature of the digital content or digital service and taking into account any public statement made by or on behalf of the trader, or other persons in previous links of the chain of transactions, particularly in advertising or on labeling; (c) is supplied along with any accessories and instructions

that the consumer may reasonably expect to receive; and (d) complies with any trial version or preview of the digital content or digital service, made available by the trader before the conclusion of the contract.

d. Default terms with regard to control of, and other data activities with regard to, the supplied data. Similar to paragraph (2)(c)(i) of this Principle, the DCSD lays down an obligation to supply the recipient with digital content or services that are free from any third-party rights. Article 10 of the DCSD provides that when a restriction resulting from a violation of any right of a third party, in particular intellectual property rights, prevents or limits the use of the digital content or digital service in accordance with the contract, the consumer shall be entitled to remedies for lack of conformity unless national law provides for the nullity or rescission of the contract for the supply of the digital content or digital service in such cases. Similar provisions can be found in national sales laws or laws of obligations (cf. Section 933 Austrian Civil Code; Article 7:15-7:16 Dutch Civil Code; Article 217(2)(4) Estonian Law of Obligations Act; Article 41(1) Finland Sales Act; Section 435 German Civil Code; Section 41 UK Consumer Rights Act).

In contracts for the sale of goods (cf. Article 10(1) CSD II, Directive (EU) 2019/771; Article IV.A – 5:102 Draft Common Frame of Reference (DCFR); Article 42 Convention on the International Sale of Goods (CISG)), the risk passes when the goods are supplied under paragraph (2)(c)(ii) of this Principle. The limitation that developments after the data has been supplied do not by themselves give rise to a claim by the recipient against the supplier can also be found in Article 11(2) of the DCSD, according to which the trader shall normally be liable only for any lack of conformity that exists at the time of supply.

As to the supplier's duties to support the recipient in complying with all legal requirements with respect to control of the data, as can reasonably be expected, including by providing information (paragraph (2)(c)(iii) of this Principle), most European jurisdictions would qualify this as an ancillary obligation under the contract. Article 1:202 of the Principles of European Contract Law (PECL) provides for a general duty for parties to cooperate. In order to give full effect to the contract, each party should perform what they owe to the other party (See also Article III. – 1:104 DCFR). European data protection law recognizes a duty of the recipient of personal data to support the supplier in complying with all legal obligations. Article 28(3) of the General Data Protection Regulation (GDPR) provides that the processor must, inter alia, assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights and in ensuring compliance with legal obligations. Furthermore, Clause 8.6(d) Module two and Module three of the Standard Contractual Clauses (SCC) (Commission Implementing Decision (EU) 2021/914) provides that the data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the GDPR.

As to the recipient's general legal position, paragraph (2)(c)(iv) of this Principle follows a "sales approach" rather than a "license approach." Hence, it is set out that the recipient is generally entitled to use the data for any lawful purpose.

The attribution of intellectual property rights for newly created content to the recipient (paragraph (2)(c)(v) of this Principle) is based on the idea that, normally, the recipient is the one who will make the essential intellectual effort for the development of these rights. Under European

law, intellectual property rights will therefore normally be vested in the recipient anyway (see Articles 2 – 4 Information Society Service Directive, Directive 2001/29/EC; Article 2(2) Rental and Lending Directive, Directive 2006/115/EC; Article 2(1) Software Directive, Directive 2009/24/EC). The policy choice to attribute newly created content to the recipient is also reflected in European contract law. According to Article 16(4) of the DCSD, the consumer can, after the termination of the contract, request any content that was created by the consumer when using the digital content or digital service supplied by the provider.

Due to its non-rivalrous nature, data can be used simultaneously by various actors without exhausting the resource. Hence, paragraph (2)(c)(vi) of this Principle provides a default rule to the effect that the supplier may retain a copy of the data and may continue using it, including by supplying it to third parties.

e. Application of other law by analogy. Since the implementation of the DCSD, the most appropriate analogy in Europe will usually be with contracts for the supply of digital content or digital services. In business-to-business (B2B) cases, the relevant rules must be distinguished from any consumer-specific policy decisions. However, national courts may, for B2B cases, also retain the solutions they developed before the DCSD was issued. Many European legal systems apply rules on sales *per analogiam* also to the supply of digital content if the recipient can use the content for an unlimited period. The provisions for lease contracts are often applied if the use is limited to a certain (albeit possibly indefinite) period and the rules for service contracts if the digital content is customized. For example, the Principles of European Law and the Draft Common Frame of Reference (DCFR) apply, with appropriate adaptations, to contracts for the sale or barter of information and data, including software and databases, except when the buyer is only given a license to use the software (see, e.g., Article 1:105 Principles of European Law, Sales; Article IV.A. – 1:101(2)(d) DCFR). The Principles of European Law further clarify that the sales provisions are also applied *per analogiam* to the transfer of information "to the extent that it is a standard affair." However, if the transaction involves a request for evaluative information, it will be classified as a service.

Principle 8. Contracts for Simple Access to Data

(1) A contract for simple access to data is one under which the supplier undertakes to provide to the recipient access to particular data on a medium within the supplier's control and which is not a contract for the transfer of data under Principle 7. This includes contracts in which the supplier, in addition to enabling the recipient to read the data, undertakes to put the recipient in a position to process the data on the medium within the supplier's control, or port data.

(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the law should provide that the following terms are included in a contract for simple access to data:

(a) With regard to the mode of the recipient's access to the data:

(i) the supplier must provide the recipient with the necessary access credentials and remove any technical barriers to access whose removal could reasonably be expected in a transaction of the relevant kind;

(ii) the supplier must make the data accessible in a structured and machine-readable format of a sort that can reasonably be expected in a transaction of the relevant kind;

(iii) the supplier must enable the data to be accessed remotely by the recipient unless this is unreasonable in light of data security concerns;

(iv) the recipient may process the data to which the recipient is given access only for purposes consistent with any purposes agreed in the contract;

(v) the recipient may port data to which the recipient is given access in the contract only when the porting of such data can reasonably be expected in a transaction of the relevant kind, and may port data derived from the recipient's processing activities carried out in accordance with the contract (e.g., data derived from data analytics); and

(vi) the recipient may read, process, or port the data, as applicable, by any means, including automated means, and may do so as often as the recipient wishes during the agreed access period.

(b) With regard to the characteristics of the data to which access is provided, the terms listed in Principle 7(2)(b) for contracts for transfer of data also apply in a contract for simple access to data.

(c) With regard to the control of any data ported by the recipient in accordance with the contract, and other data activities, the terms listed in Principle 7(2)(c) for contracts for transfer of data also apply in a contract for simple access to data.

(3) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to contracts for simple access to data, consideration should be given in particular to whether, and the degree to which, the recipient may only view the data, may process data on the medium within the supplier's control, or may port data.

Comment:

a. Scope This Principle covers contracts in which the obligation assumed by the supplier is to give the recipient access to data on a medium within the supplier's control. Parties may wish to choose a contract for simple access to data when they do not want the recipient obtaining full control of (all) the data that are the object of the bargain. This can be for data privacy/protection, data security, or other reasons, in particular in light of the fact that data that has once been transferred to a recipient can hardly be recovered if used or passed on by the recipient in breach of the terms agreed. Contracts for simple access to data do not fall under Principle 7, but are covered in this Principle (and, to a certain extent, in Principle 9). The main difference between contracts within Principle 7 and those within this Principle is that, under the latter, the supplier does not transfer the data to a medium under the control of the recipient but, rather, gives the recipient access to a medium under the supplier's control on which the data is stored.

Illustrations:

42. Car manufacturer S conducts intensive research on the development of new car models, collecting vast amounts of test data on various prototypes and their components. The data would enable engine manufacturer R to learn better how its engines operate and how they can be improved. S is willing to enter into a contract with R that would enable R to obtain that benefit but, in light of the vast investment made by S into the research and the risk that any data transferred to R will be passed on to competitors or hacked by third parties, S is reluctant to transfer the test data to R. Rather, the parties agree that R will have access to a defined class of test data on S's servers. The contract effectuating this agreement is a contract for simple access to data under this Principle.

43. Same facts as Illustration no. 42, except that the contract requires S to upload the data to R's server. The contract is a contract for the transfer of data under Principle 7.

Contracts for simple access to data can involve situations in which the recipient is provided read-only access, as well as those in which the recipient may process the data on the medium within the supplier's control, or port particular data. As the key motivation for suppliers to enter into a contract for simple access to data, covered by this Principle, rather than into a contract for the transfer of data, covered by Principle 7, is typically for the supplier to remain in full control of the data, this motivation may be best served if access is provided to the recipient on a read-only basis. However, a read-only basis is often not sufficiently useful for the recipient. This is why parties

frequently agree that the recipient is permitted not only to read the data but also to process the data on the medium within the supplier's control, or port particular data. Such contracts also fall under this Principle.

Illustration:

44. In order to benefit from the test data and be able to improve its engines, R in Illustration no. 42 would need to conduct its own research using the data. Accordingly, S and R agree that R may run its own data analytics on S's servers, thus engaging in data processing on a medium controlled by S. Because R wants to use the results of such data analytics in R's own factory, S and R agree that R may port the results of data analytics, transferring those results to R's own servers. The contract is a contract for simple access to data under this Principle.

The greater the portion of data the recipient is allowed to port, the more similar in effect the transaction will be to a contract for the transfer of data under Principle 7.

b. Default terms with regard to the mode of the recipient's access to the data. The default terms in paragraph (2)(a) of this Principle regarding the mode of the recipient's access to the data are necessarily more complex than the terms stated in Principle 7 with respect to the mode of supply.

First, because the access will typically be secure, paragraph (2)(a)(i) of this Principle states that the supplier must provide the recipient with the necessary access credentials and remove any technical barriers whose removal could reasonably be expected in a transaction of the relevant kind.

Illustration:

45. Assume that, in Illustration no. 42, S provides R with the access credentials, but when R tries to access the data, R can read the data, which is encrypted, only if R is prepared to buy special, expensive decryption software used by S but not common in R's industry. S could easily decrypt the data itself. R has a right against S that S remove the technical barrier posed by the encryption.

Second, paragraph (2)(a)(ii) of this Principle supplies a default term as to the format in which the data is to be accessible. Under that term, the data must be accessible in a structured and machine-readable format that can reasonably be expected in transactions of the relevant kind.

Third, the default term in paragraph (2)(a)(iii) of this Principle provides that the recipient may access the data remotely unless that is unreasonable in light of data security concerns. Of course, in some cases, the parties may agree that the recipient is allowed to view the data only locally, e.g., when the data is saved on a server without internet connection.

Illustration:

46. Assume that, in a situation such as the one in Illustration no. 42, when R requests remote access to S's server for the first time, S denies access, claiming that its internal security policies only allow such data to be accessed locally. Instead, S insists that R's employees must travel to S's premises whenever R intends to access the data. According to the default term in paragraph (2)(a)(ii) of this Principle, S is allowed to deny access to R only if remote access is, in light of the sensitivity of the data and the inherent insecurity of the internet connections available to R, objectively unreasonable, and not just according to S's internal policies.

Fourth, paragraph (2)(a)(iv) of this Principle provides that the recipient may process the data to which the recipient is given access only for purposes that are consistent with the purposes agreed in the contract. This default term differs from the default term provided in paragraph (2)(c) for data to be ported (the latter being the same as under Principle 7(2)(c)(iv)). The reason is that the likely primary motivation for parties to enter into a contract for simple access to data under this Principle instead of into a contract for the transfer of data under Principle 7 is that the supplier wants to remain in control, in particular due to data security or data privacy/data protection concerns, or any other necessity to remain abreast of data activities with regard to the data in question.

Illustration:

47. Assume that in a situation such as the one in Illustration no. 42, the parties originally envisaged in their contract that R would engage in certain processing activities to learn better how its engines operate and how they can be improved. However, when analyzing the data, R realizes that there is huge potential in the data for developing a new recommender system for connected cars. Given that this purpose is different from the purpose agreed in the contract, and might potentially harm S's interests (e.g., if S itself is

developing such a service), R cannot simply process the data for that purpose but has to seek an extended agreement with S.

These reservations do not apply with regard to data that the recipient may port to its own servers, which is why paragraph (2)(c) of this Principle refers to the sales approach adopted under Principle 7(2)(c)(iv) for data ported by the recipient.

Fifth, paragraph (2)(a)(v) of this Principle addresses which data the recipient is allowed to port. Given that porting data is likely to undermine the motivation of the parties for choosing a contract under this Principle instead of a contract for the transfer of data under Principle 7, this default term is rather restrictive. Under this term, the recipient may port only such data as the recipient could reasonably expect to be allowed to port in a transaction of the relevant kind. paragraph (2)(a)(v) of this Principle also supplies a default term that, if the recipient is entitled to process the data (e.g., by analyzing it) on the supplier's medium, the recipient may also port the derived data.

Illustration:

48. According to the contract between S and R in Illustration no. 42, R is allowed to run its own data analytics with its own software in a workspace on S's servers in order to learn more about the performance of its engines. However, after the data analytics have been completed and R asks S for the credentials required for porting the results, S claims that porting of any data was not part of the contract, and that R is allowed to port the results of the analytics only if R is prepared to pay a significant extra sum of money. Even if the contract is silent, R has a right to port the data derived from its own processing activities.

Sixth, paragraph (2)(a)(vi) of this Principle provides a default term that, as is typical in contracts for simple access to data, the recipient may read, process, or port the data by any means, including automated means, and as often as the recipient wishes during the agreed access period.

Illustration:

49. Assume that in a situation such as the one in Illustration no. 42, R accesses the data with the help of advanced artificial intelligence (AI), which, within only a few hours, analyzes all of the data made accessible to R. S did not anticipate this and claims that this sort of access is improper and that, if R had disclosed its intentions during the negotiations,

the price for the access would have been much higher. As the parties have left this point open, the default position is that R is entitled to access the data with the help of AI.

c. Default terms with regard to the characteristics of the data supplied. Paragraph (2)(b) of this Principle indicates that, with respect to the characteristics of the data supplied, the supplier has the same responsibilities as it would have in a contract for the transfer of data. See Principle 7(2)(b). This reflects the view that there are no policy reasons for differentiating between a contract for the transfer of data and a contract for simple access to data with respect to these issues. As with the default terms stated in paragraph (2)(a) of this Principle, the parties are free to vary from these terms by agreement.

d. Default terms with regard to legal rights and obligations with respect to any data ported by the recipient. As with the rules with respect to characteristics of data supplied, paragraph (2)(c) of this Principle indicates that the supplier in a contract for simple access to data has, as far as data ported by the recipient in accordance with the contract is concerned, the same responsibility with regard to legal rights and obligations as it would have in a contract for the transfer of data. See Principle 7(2)(c).

e. Application of other law by analogy. Principle 5 provides that default rules and principles not directly applicable to the transaction at hand but that would govern a type of transaction akin to the transaction at hand may be applied to that transaction by analogy. Paragraph (3) of this Principle provides additional guidance in the context of contracts for simple access to data. Under the law of most jurisdictions, the closest analogy will often be that of some kind of services contract, the service being to enable the recipient to access the data. However, depending on the circumstances, and in particular on the extent to which the recipient may port data, appropriate analogies may also be a sale or lease (see Principle 7).

REPORTERS' NOTES

See the Reporters' Notes to Principle 7. The existing law in the United States and in Europe does not generally distinguish between the types of contracts described in Principle 7 and this Principle.

Principle 9. Contracts for Exploitation of a Data Source

(1) A contract for exploitation of a data source is one under which the supplier undertakes to provide to the recipient access to data by providing access to a particular device or facility by which data is collected or otherwise generated (the "data source"), enabling the recipient to read, process, or port data from the data source.

(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the law should provide that the following terms in addition to those provided in Principle 8 are included in a contract for exploitation of a data source:

(a) With regard to the mode of the recipient's access to the data on the data source:

(i) the recipient may port all data collected or generated by the data source; and

(ii) access to the data is provided in real time as the data is collected or generated by the data source.

(b) With regard to the characteristics of the data, there is no requirement that the recipient receive data of a particular quality or quantity.

(3) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to contracts for exploitation of a data source, consideration should be given in particular to:

(a) the degree and duration of control that the recipient is to receive over the data source; and

(b) whether, and the degree to which, the recipient may port data.

Comment:

a. Scope. Under a contract for exploitation of a data source within the meaning of this Principle, the supplier undertakes to provide to the recipient access to data by giving the recipient access to a device or facility by which data is collected or otherwise generated. A contract for exploitation of a data source is thus a special type of a contract for access to data, focusing on access to, and usually processing and/or porting of, data collected or generated by the data source. Thus, the focus of the transaction is the data source rather than the characteristics of the data. If a contract is about access to particular (existing) data, it is not a contract for exploitation of a data

source addressed by this Principle, but a contract for the simple access to data under Principle 8. Contracts for the exploitation of a data source are common in the data economy.

Illustrations:

50. Car manufacturer C makes a contract with business B under which B is granted access to the data generated by the connected cars' windshield wipers and headlights, which in turn enables B to provide exact weather reports even for areas where no other weather sensor data is available. Neither C nor B know how much the car owners will drive their cars and where and when they will drive them, and C does not make any promise to B in that regard. Because B is granted access to the facility by which data is produced and the contract is not one for access to data under Principle 8, the contract is one for exploitation of a data source.

51. Company N runs a news website. Use of the website by every visitor is, under contractual agreements with N, closely monitored and recorded by data broker B. B will use the data for profiling and scoring purposes. The agreement between N and B is a contract for exploitation of a data source because neither N nor B knows exactly how many visitors will use the website and there is no requirement that there be any particular number of visitors.

The technical arrangements for providing the recipient with access to the device or facility as described in paragraph (1) may vary. In particular, it is not necessary that the supplier gives the recipient access to the "original" data source. Very often, the parties will agree that the data may be transferred from the original data source to a kind of "duplicate" of that source, to which the recipient is then provided access.

Illustration:

52. In a case such as the one described in Illustration no. 50, car manufacturer C does not wish to give B direct access to its car fleet. Rather, the parties agree to an arrangement under which C initiates automatic and continuous transfer of any data generated by the windshield wipers and headlights to a server space to which B is then granted access. While this server space is not really the "data source," the parties have made it a "duplicate" of the original data source. Accordingly, the contract is one for exploitation of a data source.

b. *Default terms.* The default terms included in a contract for exploitation of a data source are, as a starting point, the same as under Principle 8. However, there are three additional terms complementing or concretizing the terms listed in Principle 8(2). In particular, when the default terms in Principle 8(2) refer to what can "reasonably be expected in a transaction of the relevant kind," the fact that the nature of the transaction is one for exploitation of a data source rather than one for access to particular data is relevant in determining those reasonable expectations. More precisely, in a contract for exploitation of a data source under this Principle, there are two specific default terms, i.e., that the recipient is (i) permitted to access and port all data generated by the data source, and (ii) given real-time access to the data as the data is generated, or as close to real-time access as is reasonably possible.

Illustrations:

53. Assume that, in Illustration no. 52, a certain part of the data generated by the windshield wipers is not transferred by car manufacturer C to the medium made accessible to B because C is afraid that this part of the data might disclose details about a new feature C is developing (activation of windshield wipers by the driver's facial expression). Unless this was agreed between B and C, pruning the data by C would be in breach of the default terms incorporated under paragraph (2)(a)(i) of this Principle.

54. Assume further that, in Illustration no. 52, a certain part of the data generated by the windshield wipers is made available to B only with a time lag of up to 30 minutes. Unless this was agreed between B and C, this deviation from real-time access would be inconsistent with the reasonable expectations of parties in a transaction of this kind and C would be in breach of the default terms incorporated under paragraph (2)(a)(ii) of this Principle.

Another key difference between contracts for simple access to particular data under Principle 8 and contracts for exploitation of a data source under this Principle concerns terms as to the characteristics and quantity of data: Unless the parties have agreed otherwise, the supplier in a contract governed by this Principle has no obligation with respect to the quality or quantity of data to which the recipient will have access. Of course, parties will sometimes deviate from this default rule and agree, e.g., that the recipient will be enabled to harvest a particular minimum quantity of data and/or data of a particular minimum quality. But if both the quality and the quantity of data are clearly defined in the agreement, the transaction would often be one in which the recipient is

granted access to "particular data" and the contract would be subject only to Principle 8. It is worth noting that the terms listed in Principle 7(2)(b) and incorporated in Principle 8(2)(b) still apply, and thus, for example, material descriptions or representations would still be relevant.

Illustration:

55. Assume that, in Illustration no. 50, business B approaches car manufacturer C, describes to C its plans to develop a smart weather report service for remote areas, and asks C whether there is any data generated by C's cars that would be suitable for this purpose. C then offers to B access to the connected cars' windshield wipers and headlights, to which B agrees. It turns out, however, that the headlights do not at all react to different weather conditions, but run in the same mode irrespective of whether rain is pouring or the sun shining, and that the windshield wipers are automatically activated also when there is dust on the windshield, rendering the windshield wiper data much less useful for B's purposes. As C had notice of B's particular purpose for obtaining the data and that B was relying on C's skill or judgment in selecting the data source, the data source must be fit for the recipient's particular purposes. However, unless the parties have agreed otherwise, B would not be entitled to a particular quantity of headlight or windshield wiper data and, for example, B would not have any rights against C if it turns out that buyers of C's cars are becoming more climate-aware and use their cars less often.

As to terms with regard to control or use of any data ported by the recipient in accordance with the contract, the same default rules apply as under a contract for access to data under Principle 8.

Illustration:

56. In Illustration no. 51, company N would be under an obligation vis-à-vis B to seek valid consent from the visitors to the website or to ensure otherwise that relevant data privacy/data protection legislation is complied with. However, unless otherwise agreed, N has no obligations with respect to the number of clicks from visitors.

c. Application of other law by analogy. Contracts for access to a data source do not readily analogize to other well-developed sets of contract law rules. A functional analogy might be that of a lease of the medium, device, or facility to which the recipient is granted access, when the recipient gets a significant degree of (temporary) control over that source. This device or facility is often

owned or otherwise run by the supplier, so if the supplier contracts for the use of that facility by the recipient for the purpose of collecting and further processing data, it is not far-fetched to analyze this as a form of lease or a contract akin to a lease. This analysis may be useful when, for instance, a court needs to fill a gap in the contract.

Illustration:

57. In Illustration no. 51, company N enters into a contract with B to allow it to use the news website, for a specified amount of time, for monitoring and recording the browsing behavior of visitors. N's obligation vis-à-vis B to enable it to pursue its activities during that time period could be analogized to the obligation of a lessor to enable a lessee to use a leased facility. Accordingly, should B claim that it accessed the data only during a small portion of that time, and thus should not have to pay for the portion of the access period that it did not utilize, that claim would not succeed, just as a lessee of a facility must pay the full lease price without regard to how often it used the facility during the term of the lease.

In jurisdictions where there is a difference between such lease contracts in which the lessee is allowed only to use the leased object, and lease contracts in which the lessee may derive and keep the fruits of the leased object (such as the crop yielded by a farm or the profit yielded by a restaurant) the appropriate analogy would be rather the latter, depending on whether and to what extent the recipient is allowed to port and keep data.

REPORTERS' NOTES

United States:

As to the absence of a default term about the quantity of data that will be involved, an analogy may be drawn between the sort of transactions covered by this Principle and output contracts governed under the law of sales. See Uniform Commercial Code (UCC) § 2-306 (2021-2022 ed.). See also Restatement of the Law Second, Contracts, Introductory Note to Chapter 11 (AM. L. INST. 1981) ("The obligor who does not wish to undertake so extensive an obligation may contract for a lesser one by using one of a variety of common clauses: . . . he may restrict his obligation to his output or requirements . . . .").

As to the absence of a default term with respect to the quality of the data, an analogy may be drawn to "as is" sales under UCC § 2-316, which contain no implied warranties. While an explicit phrase such as "as is" can exclude such warranties under UCC § 2-316(3)(a), such warranties may also be excluded by the commercial context as shown by course of dealing, course of performance, or usage of trade. See UCC § 2-316(3)(c).

Europe:

It is typical for contracts for the lease of a particular device under the laws of the various European jurisdictions that implied warranties refer to the item made available to the lessee, and not to the benefits the lessee will ultimately derive from the leased item (see Section 1090 ff Austrian Civil Code; Section 1719 ff French Code Civil; Section 535 ff German Civil Code). Some jurisdictions stress objective standards for the conformity of the leased items, such as Section 1720(1) of the French Code Civil, stating that the lessor has to deliver the goods "in a good state of repair in all respects." Other jurisdictions refer to the "agreed use" and focus more on subjective standards (cf. Section 1096 Austrian Civil Code; Section 535(1) sentence 2 German Civil Code). Other jurisdictions follow a mixed approach (cf. Section 592 Slovenian LOA: "agreed or customary use"). In many jurisdictions, a difference is made between contracts about items that are only for the lessee's use (e.g., a residential apartment) and contracts about items that are for economic exploitation by the lessee (e.g., a restaurant). In particular, in the latter case, it is often difficult to draw a clear line between the features of the leased items, which are part of the lessor's contractual obligations, and the lessee's expected benefit from the use, which is entirely at the risk of the lessee.

Principle 10. Contracts for Authorization to Access Data

(1) A contract for authorization to access data is one under which the supplier (referred to in this Principle as the "authorizing party") authorizes the access to data or a data source by the recipient, including usually processing or porting of the data, but when, in light of the passive nature of the authorizing party's anticipated conduct under the contract and the authorizing party's lack of meaningful influence on the transaction, the authorizing party cannot reasonably be expected to undertake any responsibilities of the sort described in Principles 7 to 9.

(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the law should provide that in a contract for authorization to access data:

(a) with regard to the mode of the recipient's access, a term that the authorizing party will facilitate or assist the recipient in gaining access is not included, and the authorizing party may continue using the data or data source in any way, even if this impairs the recipient's access or even renders it impossible;

(b) with regard to the characteristics of the data, there is no requirement that the recipient will receive data of a particular quality or quantity;

(c) with regard to control of the data and any other data activities the recipient may engage in, the authorizing party has no obligation to ensure that the recipient will have any particular rights;

(d) as between the authorizing party and the recipient, the recipient is responsible for compliance with any duties vis-à-vis third parties under Part IV, including the duties incumbent on a supplier of data under Principle 32; and

(e) the recipient must indemnify the authorizing party for any liability vis-à-vis third parties that follows from the authorizing party's authorization to access the data unless such liability could not reasonably be foreseen by the recipient.

(3) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to contracts for authorization to access data, consideration should be given to whether the focus of the agreement between the parties is on the access to the data or on the supply of another commodity (such as a digital service) in the course of which access to the data occurs.

Comment:

a. Scope. This Principle addresses data transactions in which the authorizing party provides the recipient with access and allows processing but undertakes no obligations with respect to that data. In contrast to a contract for access to particular data under Principle 8 or for access to a data source under Principle 9, the authorizing party does not in any way undertake to support the recipient in accessing or processing the data, or to remove any technical or legal barriers.

b. Default terms. As set out in paragraph (2), the default terms in a contract for authorization to access are rather minimal, putting no obligations on the authorizing party. In particular, subject to contrary agreement of the parties as far as such contrary agreement is consistent with mandatory law (see Principle 5), the supplier (who, in order to contrast the position of the parties in the contracts governed by this Principle with those covered by Principles 7 to 9, is referred to as the "authorizing party") does not undertake to facilitate or assist the recipient in gaining access. Also, the authorizing party may continue using the data or data source (e.g., an electronic device) as the authorizing party wishes, even if this impairs the recipient's access or renders it impossible (e.g., because the device is disconnected from the internet). Accordingly, the authorizing party does not warrant that the recipient will receive data of a particular quality, fitness for purpose, or quantity, nor that the recipient will have a particular legal position with regard to the data.

Illustration:

58. Provider M provides a messenger application and service "for free." In return, users authorize the processing of personal data on the device on which the application is installed for a variety of purposes that are in M's commercial interest. In this passive access situation, the users are under no obligation actually to use the messenger service, to produce a minimum quantity of user-generated data, or to produce data of a particular quality (e.g., data that reveals the actual identity of the individuals with whom the users correspond). Users are also free to delete the application, thus making any further access to the data source on the part of M impossible.

c. Duties with respect to third parties. Unlike the contracts described in Principles 7 to 9, in which the default terms primarily impose duties on the supplier, this Principle contains default terms that impose significant duties on the recipient. If the authorizing party were to qualify as a normal "supplier," it would be subject both to any duties it owes vis-à-vis third parties under Principle 32 and to potential liability when those duties are breached; but in a contract for authorization to access, those costs should not ordinarily be borne by the authorizing party, whose role is quite passive. Accordingly, paragraph (2)(d) of this Principle supplies a default term stating that the recipient is, as between the authorizing party and the recipient, responsible for complying with the duties under Principle 32. Also, under paragraph (2)(e) of this Principle, the recipient must indemnify the authorizing party for any liability vis-à-vis third parties that follows from authorization to process data unless such liability was not reasonably foreseeable by the recipient.

Illustration:

59. Assuming that provider M in Illustration no. 58 not only instigates user C to permit processing of C's own personal data, but also to "authorize" the processing of personal data of all individuals displayed under C's contacts on the mobile device. Even though it is still primarily C who remains responsible vis-à-vis his friends, M has to assume responsibility for making sure C is allowed to pass on his friends' data, and for complying with all duties under Principle 32; and in case C is sued by one of his friends, to indemnify C for all liability.

d. Application of other law by analogy. In deciding which law to apply by analogy within the meaning of Principle 5, the focus of the parties' agreement should be considered. In some

transactions, access to the data may be the main subject matter of the agreement. More often, however, access to the data is not what the agreement, as reflected in the parties' declarations and any contract documents, is mainly about, but, rather, is an incidental element within a wider transaction about something else, such as provision of some digital service (e.g., search engine service, navigation service, messenger service) by the recipient of the data to whom authorization to access is granted. When this is the case, authorization to access is best seen not as the defining characteristic of the transaction but, rather, as a substitute for payment in money for the digital service.

Illustrations:

60. In Illustration no. 58, user C allows provider M to use C's devices (e.g., a mobile phone and messenger application) for the collection of personal data. A court might, when relevant in a domestic legal system, analyze this as a case of consideration other than money.

61. Farm corporation F buys a "smart" tractor from seller S, which has been manufactured by manufacturer T. The tractor comes with digital services, including weather forecasts, soil analyses, targeted recommendations concerning the use of particular fertilizers and insecticides, and predictive maintenance, to be provided by T and companies U and V that cooperate with T. T, U, and V will normally use the data that is collected by the sensors of the tractor for their own commercial purposes. Economically speaking, T, U, and V will consider the value of the data they will probably receive, and the profits they can derive from exploiting the data, when calculating the price to be charged for the tractor and any digital service provided.

The insight that authorizing the processing of user-generated data amounts to a form of payment, at least from an economic point of view, may be relevant in a number of different contexts. For example, when a jurisdiction provides different rules for gratuitous contracts and for non-gratuitous contracts, the fact that data is provided in lieu of a sum of money may mean that the contract should be treated as a non-gratuitous contract.

REPORTERS' NOTES

United States:

As to the basic default terms, see the Reporters' Notes to Principles 7 through 9.

Some of the matters in this Principle are addressed from a different perspective in Principles of the Law, Data Privacy § 5 (AM. L. INST. 2020). That Section addresses the nature of the consent necessary on the part of the authorizing party to enter into a transaction of this sort. That Section requires that "When consent is required, [the authorizing party] shall be given understandable and easy-to-use means to permit exercise of meaningful choice in relation to personal data activities regarding the [authorizing party's] personal data." Id. § 5(b). Further, the authorizing party must be provided reasonable notice, and consent may not be obtained in a misleading or deceptive fashion. Id. § 5(e) and (f). Additionally, the form by which consent is obtained must be reasonable under the circumstances. Id. § 5(g)(1). Finally, the authorizing party may withdraw consent, subject to legal or otherwise reasonable restrictions, by providing reasonable notice to the recipient. Id. § 5(h).

Europe:

a. Scope. In Europe, there is much awareness of the phenomenon of businesses collecting data, in particular (but not exclusively) personal data, from their contracting partners for commercial purposes. Often, but not always, this occurs in the context of a contract for digital services that is purportedly provided "for free," while really the business is providing the service in return for the data collected. Recently, this phenomenon has spread far beyond "pure" digital services such as search engines, messenger services, or social media, to the tangible world. For example, many fleets of electrical scooters for hire in bigger cities are said to be run exclusively with the purpose of collecting mobility and other relevant data, as it is clear from the outset that the rather nominal monetary fees charged for hiring the scooter will suffice to amortize the purchase price during the scooter's short lifespan. In legal terms, this phenomenon has been discussed as "data as counter-performance" or "data as consideration." It was first addressed openly by the European legislator in the 2011 Common European Sales Law (CESL) Proposal, and later in the 2015 Proposal for a Directive on contracts for the supply of digital content (COM(2015) 634 final). Article 3(1) of that Proposal stated that the proposed Directive should apply to any contract in which the supplier supplies digital content to a consumer and, in exchange, a price is to be paid "or the consumer actively provides counter-performance other than money in the form of personal data or any other data." After the European Data Protection Supervisor (EDPS), in the famous Opinion No. 4/2017, had compared the concept to trade in live human organs and stated that the catchphrase of "paying with data" could be dangerous if turned into a legal principle (No. 17 (with endnote 27) of EDPS Opinion 4/2017), the wording was changed. The final version of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) now makes payment of a price or provision of data by the consumer beyond what is necessary for the fulfilment of the contract or of legal duties an objective requirement for the Directive's legal regime to apply, thus avoiding any explicit classification of data as "counter-performance," while the underlying idea remains the same (Article 3 DCSD). The notion has now been extended to the Consumer Rights Directive (see Article 3(1a) Directive 2011/83/EU, as recently adapted by Directive (EU) 2019/2161). The immediate consequence is that a consumer has the same rights (with regard to information, a right of withdrawal, or remedies for lack of conformity) irrespective of whether a price is paid in money or whether data is provided.

b. Default terms, *c. Duties with respect to third parties*, and *d. Application of other law by analogy*. Before the wording was changed, and while data was still explicitly classified as "counter-performance," there was a lively academic debate concerning the consumer's duties and potential liability for breach, e.g., if the consumer withdraws their consent to the processing of personal data, or provides poor data quality (such as a fake name), or fails to make sure other affected individuals have given consent to the processing of their data (see Axel Metzger, Data as Counter-Performance – What Rights and Duties do Parties Have?, JIPITEC 2017, 6). While the academic debate is still ongoing, it has arguably been overtaken by political developments. Given that the European legislator clearly changed its strategy and no longer qualifies data as "counter-performance" or "consideration" but rather insists that data protection is an inalienable human right, any liability of the consumer for breach, or even more so an enforceable obligation to provide data, should be off the table. However, the DCSD leaves it as a matter of national law to set out the consequences for the contract in the event that the consumer withdraws the consent for the processing of the consumer's personal data (Recital 40 DCSD; on the consequences, see, inter alia, Section 327q German Civil Code; Sebastian Schwamberger, Die Folgen eines datenschutzrechtlichen Widerrufs bei Verträgen über digitale Leistungen, ecolex 2021, p. 795). In any case, national law can only provide for consequences that are consistent with the GDPR.

Principle 11. Contracts for Data Pooling

(1) A contract for data pooling is one under which two or more parties (the "data partners") undertake to share data in a data pool by:

(a) transferring particular data to a medium that is jointly controlled by the data partners or that is controlled by a data trustee or escrowee or other third party acting on behalf of the data partners; or

(b) granting each other access to particular data or the possibility to exploit particular data sources, with or without the involvement of a third party.

(2) This Principle applies, with appropriate adjustments, to the governing principles of any entity created pursuant to a data pooling contract.

(3) Subject to agreement of the parties and to rules that take priority pursuant to Principle 5, the law should provide that the following terms are included in a contract for data pooling:

(a) A data partner may utilize data from the data pool, or data derived from such data, only

(i) for purposes agreed upon between the data partners in the contract for data pooling;

(ii) for purposes that the relevant data partner could reasonably expect to be accepted by the other data partners, unless these purposes are inconsistent with an agreement referred to in paragraph (3)(a)(i); or

(iii) as necessary to comply with applicable law.

(b) A data partner may engage data processors, but may otherwise pass data from the data pool, or data derived from such data, on to third parties only under the conditions agreed upon between the data partners or required by applicable law.

(c) As between the data partners, new intellectual property rights or similar rights created with the use of data from the data pool belong to the partner or partners who conducted the activity leading to the creation of the new right.

(d) If a data partner leaves the data pool, the data supplied by that data partner must be returned to the relevant data partner, but data derived from that data, unless essentially identical with the data originally supplied by that data partner, remains in the pool. Upon leaving the data pool, a data partner is entitled to a copy of any data in the pool that has been derived, in whole or in substantial part, from data originally supplied by that data partner.

(4) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to contracts for data pooling, consideration should be given to whether the relationship between the data partners is one characterized by mutual trust and confidence, such that the data partners owe each other fiduciary obligations, or, rather, whether it is characterized by arm's length transactions with no fiduciary obligations.

Comment:

a. Scope. This Principle applies to a phenomenon under which separate parties, which are here called the "data partners," agree to share data in a way that there is not a "supplier" and a "recipient" but that each of the parties is, at the same time, both supplier and recipient with regard to data shared in a data pool. Often, such arrangements are referred to as "closed data platforms," with "closed" indicating that the data pool is accessible only to the data partners involved and not to a wider public, such as under open data schemes. The technical and legal arrangements in place may vary. Very often, the data partners will transfer data to a medium (or a defined sector of such a medium, such as cloud space) that is controlled jointly by all partners or by a third party. The third party may, in particular, be a "data trustee" within the meaning of Principle 13, or an

"escrowee" within the meaning of Principle 14, or a new company established and held jointly by the data partners specifically for the purpose of managing and exploiting the data pool. But it is also possible that the data pool is held in a decentralized manner on media controlled by each of the data partners, who then give access to that data to the other data partners within the meaning of Principle 8. Often, the data partners will focus on the exploitation of particular data sources within the meaning of Principle 9 rather than on particular data. All these arrangements may be classified as contracts for data pooling.

Illustration:

62. Tractor manufacturers M, N, and O agree to pool, and therefore to grant each other access to, a particular type of data generated by their respective smart tractors with the aim of better enabling each of them to provide a smart service, such as recommendations as to optimal use of insecticides, to farmers. If M, N, and O transfer particular data sets from the past to a server controlled jointly by M, N, and O, this is a contract for data pooling based on data transfer (Principle 7). If M, N, and O provide each other with access credentials to particular data sets stored on their respective servers, this is a contract for data pooling based on data access (Principle 8). If M, N, and O promise each other access to all the data produced by their fleet of tractors, which will be transferred in real time to a server controlled jointly by M, N, and O, this is a contract for data pooling based on exploitation of data sources (Principle 9).

b. Default terms. As with other contracts addressed in this Chapter, parties to contracts for data pooling will likely negotiate and draft contractual language to cover important business terms, but it may still be essential to determine the parties' rights and responsibilities with respect to matters that were not the subject of explicit agreement. Paragraphs (3) and (4) of this Principle address some of these issues.

The application of paragraph (3) depends on which of the three types of data pooling contract is present. In cases in which the contract provides for the transfer of data to a closed platform that is jointly controlled by the data partners or that is controlled by a third party acting on behalf of the data partners, the default rules in Principle 7 are applicable. In cases in which the contract provides for the parties granting each other access to the data, the default rules in Principle 8 are applicable. Finally, in cases in which the contract provides for the parties granting each other

the right to exploit particular data sources, the default rules in Principle 9 are applicable. In addition to incorporating default rules from Principles 7 to 9, paragraph (3) adds four more default rules.

First, in contrast with the "sales" approach chosen by Principle 7 and, as far as data rightfully ported are concerned, by Principles 8 and 9, this Principle opts for a "license" approach. This means that a data partner may utilize data from the data pool only for the purposes agreed upon between the data partners or required by law. As the parties may not be able to think of all eventualities, paragraph (3)(a) clarifies that a data partner may also use data from the data pool for purposes that data partner could reasonably expect to be accepted by all the other data partners.

Illustration:

63. Assume that M, N, and O in Illustration no. 62 agree that the pooled tractor data may be used for improving the databases for an enumerative list of precision farming services. N decides to engage also in real estate services, arranging deals between buyers and sellers of farmland and providing services in this context. Without an additional agreement between M, N, and O to that end, N would not be allowed to use data from the data pool (other than the data N itself contributed) for this new purpose. N would not be able to rely on a reasonable expectation that the other partners would accept this, as it significantly enhances the data pool's utility for N, at the expense of M and O, which might have had similar plans, or might even get into trouble with the farmers using their tractors. If, on the other hand, N wishes to report on the new data pool at its annual shareholder meeting and to show some slides with statistical data derived from the data in the pool, and the data does not disclose anyone's business secrets, N could reasonably expect that this would be accepted by M and O.

Second, in line with this "license approach," paragraph (3)(b) states that a data partner may engage data processors, but may otherwise pass data from the data pool, or data derived from such data, on to third parties only under the conditions agreed upon between the data partners or mandated by law. After all, it can be expected that the data partners are agreeing to share among themselves and would want the right to prevent others who are not parties to the contract from obtaining access to the data.

Third, the default rules in paragraph (3)(c) address the topic of ownership of new intellectual property rights or similar rights created with use of the shared data. Paragraph (3)(c) provides, as a default rule, that new intellectual property rights or similar rights created with the

use of data retrieved from the platform shall belong, as between the data partners, to the partner or partners who conducted the activity leading to the creation of the new right. With this as a default rule, the parties will have an incentive to bargain explicitly if they want a different allocation of such new rights. While paragraph (3)(c) provides a default rule for ownership of those new rights, it should be noted that applicable intellectual property law might require the parties to execute an instrument transferring those rights from whoever would own them under that law to those who are to own them under the contract.

Illustration:

64. Assume that N and O in Illustration no. 62, with the help of data from the pool and in line with the purposes agreed upon between all three partners, develop, with the help of their respective research and development departments, a new smart service with significantly more granular recommendations as to the type and optimal amount of insecticides required. As between the three data partners, the intellectual property rights in this new smart service (the type of which, such as copyright or a patent right, would depend on the applicable intellectual property regime) would belong to N and O, who have invested in the development of the new service, unless M, N, and O have agreed otherwise. If the applicable intellectual property regime assigns rights in a different manner, there would, by default, be a contractual obligation to bring the situation, as between the data partners, into line with paragraph (3)(c).

Fourth, paragraph (3)(d) together with Principle 4(2) provides that if a data partner leaves the data pool, the data supplied by that data partner must be erased. Upon leaving the data pool, a data partner is entitled to a copy of any data in the pool that has been derived, in whole or to a substantial part, from data supplied by that data partner. (Naturally, when the whole data pooling contract is terminated and all data partners leave the pool, this applies to all of the partners.).

Illustration:

65. Assume that O in Illustration no. 62 decides to leave the data pooling contract, which is silent as to the further destiny of the data. In this case, paragraph (3)(d) provides that the data generated by all smart tractors produced by O must be returned to O and must be erased from the pool. If data has been derived from that data, and the derived data is not essentially identical to the data contributed by O (such as in Illustration no. 64 in which O's

data has been aggregated with N's data to create added value) the derived data may remain in the pool, but O is entitled to a copy.

c. Application of other law by analogy. When deciding which other law to apply—either directly or by analogy—the first question that needs to be asked is whether or not a company under company law has been established, in which case many issues, such as the contributions to be made by the partners, and the benefits to be derived by the partners, would be regulated directly by company law. Generally speaking, consideration should be given to whether the relationship between the data partners is one characterized by mutual trust and confidence, such that the data partners owe each other fiduciary obligations, or, rather, whether it is characterized by arm's length transactions with no fiduciary obligations.

REPORTERS' NOTES

United States:

Data pools can be further divided into public data pools and private data pools.

> Public data pools co-mingle data assets from multiple data holders—including companies—and make those shared assets available on the web. Pools often limit contributions to approved partners (as public data pools are not crowdsourcing efforts), but access to the shared assets is open, enabling independent uses. Nonetheless, the pools are usually developed primarily to provide utility to contributing partners or other user groups such as medical researchers or humanitarian actors.

Stefaan G. Verhulst, Andrew Young, Michelle Winowatan & Andrew J. Zahuranec, *Leveraging Private Data for Public Good: A Descriptive Analysis and Typology of Existing Practices*, GOVLAB 24 (2019), available at https://datacollaboratives.org/static/files/existing-practices-report.pdf.

By way of contrast, in private data pools, "Partners from different sectors pool data assets in a controlled and restricted access environment. Unlike public data pools, this approach limits data contribution and data access to only approved partners. Private data pools tend to be highly topic-specific with development and maintenance aimed at serving a particular user group." Id. at 26.

Europe:

a. Scope. In Europe, data pooling arrangements are usually treated as a form of "data sharing" (cf. Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era', 2019, p. 9). Compared with other data sharing arrangements, the distinctive feature of data pooling is that there is not one party who is the supplier and one party who is the recipient, but instead each party is both supplier and recipient at the same time. There

is no generally recognized terminology for such arrangements, and they may equally be described, e.g., as "closed platform" or "data-sharing partnership," but they are rather common (cf. Organisation for Economic Co-operation and Development (OECD), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 46 f.). Some authors have defined data pooling as an agreement whereby companies share data "in reference to a given service or generally in an industry, or within an e-ecosystem" (see Björn Lundqvist, Competition and Data Pools, (2018) Journal of European Consumer and Market Law 4, p. 146; Heiko Richter and Peter R. Slowinski, The Data Sharing Economy: On the Emergence of New Intermediaries, (2019) International Review of Intellectual Property and Competition Law 50, p. 4, 11). The European Commission has described "data exchange in a closed platform," set up either by one core player in a data sharing environment or by an independent intermediary, as one of the standard forms of business-to-business data sharing (see SWD(2018) 125 final, p. 5).

b. Default terms and *c. Application of other law by analogy.* Since the datasets in a data pool are digital assets that come from different data partners and are used—at least to some extent—with a common interest, similarities can be drawn to the assets of a company (partnership). Comparable provisions to default rules set out by this Principle can therefore be found in European company law. Comparable to paragraphs (3)(a) and (3)(b) of this Principle, national laws limit the use of company assets by individual partners. For example, the partner of a German General Partnership may not dispose of their share of the company's assets and of the individual items belonging thereto (Section 719 BGB). For Austrian General Partnerships, Section 122(2) of the Commercial Code (UGB) provides that a partner may not withdraw company assets without the consent of the other partners.

National provisions on the retirement from and dissolution of partnerships have inspired the default rule that a partner leaving the data pool should be returned any data that was supplied. For example, the German Civil Code stipulates that all objects that the withdrawing partner has left to the partnership shall be returned (Section 738 BGB). A similar default rule can be found in the Austrian Commercial Code (see Section 137(1) UGB). In France, Article 1844-9 Code Civil provides that after payment of the debts and repayment of the share capital, the division of the assets is carried out between the partners in the same proportions as their participation in the profits, unless otherwise stipulated or agreed.

CHAPTER C
CONTRACTS FOR SERVICES WITH REGARD TO DATA

Principle 12. Contracts for the Processing of Data

(1) A contract for the processing of data is one under which a processor undertakes to process data on behalf of the controller. Such processing may include, inter alia:

(a) the collection and recording of data (e.g., data scraping);

(b) storage or retrieval of data (e.g., cloud space provision);

(c) analysis of data (e.g., data analytics services);

(d) organization, structuring, presentation, alteration, or combination of data (e.g., data management services); or

(e) erasure of data.

(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the law should provide that the following terms are included in a contract for the processing of data:

(a) the processor must follow the controller's directions, including by allowing the porting of data at the controller's request at any time, and act consistently with the controller's stated purposes for the processing;

(b) the processor must ensure at least the same level of data security and of protection for the rights of third parties as the controller was under an obligation to ensure, and must support the controller in complying with any legal obligations for the protection of third parties that could reasonably be expected in a situation of the relevant kind or of which the processor had notice when the contract was made;

(c) the processor must not pass the data on to third parties;

(d) the processor may not process the data for the processor's own purposes, except to the extent reasonably necessary to improve the quality or efficiency of the relevant service, so long as this does not harm the controller's legitimate interests and is not inconsistent with obligations for the protection of third parties within the meaning of paragraph (2)(b); and

(e) upon full performance or termination of the contract, the processor must transfer to the controller any data resulting from the processing that has not already been transferred. The processor must subsequently erase any data retained, except to

the extent reasonably necessary for existing or likely litigation or to the extent that the processor has a legal right or obligation independent of these Principles to keep the data beyond that time.

(3) In determining which rules and principles to apply directly or by way of analogy, as provided in Principle 5, to contracts for processing of data, consideration should be given to the nature of the service, such as to whether the focus is on changing the data or on keeping it safe.

Comment:

a. Scope. Contracts for the processing of data, as described in paragraph (1), are common. Given the broad definition of "processing" under Principle 3(1)(c), these contracts may appear in an extremely broad variety of forms. Contracts for processing of data may relate to the collection and recording of data (e.g., data scraping), to its storage or retrieval (e.g., cloud space provision), to its organization, structuring, presentation, alteration, or combination (e.g., data management services), to analysis of it (e.g., data analytics services), or to its erasure.

Illustration:

66. Real property business C hires the services of company P to create digital twins of C's buildings for facilitating maintenance. This includes the processing of a broad range of data, including data collected by a variety of sensors in the buildings and photographic data collected by drones. In this situation, C defines the means and purposes of the collecting and other processing of the data, and P's motivation for processing the data is to fulfill its contract with C, so C is the controller, and P qualifies as a processor, and the contract is one for the processing of data within the meaning of this Principle.

The description of "contract for processing" in paragraph (1) of this Principle should be read in conjunction with the limitation in Principle 2(1) to matters for which the "primary focus . . . is on records of large quantities of information as an asset, resource, or tradeable commodity." Accordingly, although paragraph (1) of this Principle could be read in isolation as covering some contracts involving the processing of data but in which the focus of the transaction is not related to these Principles (e.g., a photographer's services, proofreading a manuscript, etc.), such contracts are not within the scope of this Principle.

In light of the broad definition of "processing" under Principle 3(1)(c), situations in which a contracting partner engages in processing activities while fulfilling contractual duties will be common even within the general scope of these Principles. However, this Principle should apply only when the focus of the agreement is on the processing activities as such, not when processing is necessary merely to fulfill an obligation of a different nature. For example, when the operator of a data marketplace contract within the meaning of Principle 15, in order to fulfill its obligations under the data marketplace contract by facilitating a transaction between the client and other parties, processes some data provided by the client (e.g., in order to transfer it to the client's contracting party), this still should be treated as a contract under Principle 15, and not under this Principle; however, as far as the processing activities are concerned, the default terms under this Principle might still prove to be useful. When, on the other hand, data storage and storage management are important aspects of the contractual obligations of a data trustee within the meaning of Principle 13, it may be justified to apply both this Principle and Principle 13 for the respective aspects of the bundle of obligations.

b. Default terms applicable to contracts for processing of data. Paragraph (2)(a) is straightforward—a contract for the processing of data has, as a default term, an obligation of the processor both to follow the controller's directions and to act consistently with the controller's stated purposes for the processing.

Illustration:

67. If, in a situation such as the one in Illustration no. 66, real property business C directs company P not to create a digital twin of a particular building (e.g., because of security concerns raised by a state authority that is a tenant in that building), P must comply with that direction, even if there is no explicit clause to that end in the contract. Whether or not P has a claim to be paid for creating a digital twin of that building, if the building was included in the initial contract, is a different question and depends on the applicable contract law.

Under this default term, the controller may also direct the processor to port the data to another processor. However, the parties are free to agree on a fee for the porting of the data, due to the very nature of the default terms and the hierarchy stated in Principle 5. While the Principles give the controller the right to port data at any time, it should be noted that applicable contract law

might require the controller to fulfill its part of the contract, before the processor is obliged to transfer the data to another person.

Illustration:

68. Real estate company C in Illustration no. 66 has engaged cloud provider D for the storage of the data. After two months, C wants to switch to cloud provider E, as E also offers data analysis services in addition to data storage and this all-around package better suits C's needs. If C and D didn't agree otherwise, D is obliged under the default term in paragraph (2)(a) to immediately transfer the data to E, if C makes that command.

In the event of a conflict, the controller's directions typically should prevail, but when the processor is more sophisticated and realizes that the controller's directions are inconsistent with the purpose, the processor may reasonably be expected to notify the controller.

Under paragraph (2)(b), the processor has a duty to provide the same level of data protection and data security for protecting the rights of third parties as the controller is under an obligation to ensure, and similarly must support the controller in complying with its legal obligations in this regard. Generally, these duties are present only if such obligations could reasonably be expected in a situation of the relevant kind or if the processor had notice of the controller's obligations.

Illustration:

69. Assume that C in Illustration no. 66 may create a digital twin of all buildings, but is under an obligation vis-à-vis a state authority that is a tenant of one of C's buildings to treat any data of that building with a particular degree of data security. If P has notice of these requirements when the contract is made, or if the requirements could reasonably be expected, P is under an obligation to apply the same level of security to the data produced.

Paragraph (2)(c) provides that the processor must not pass data on to third parties because such action by the processor may harm the legitimate interests of one or both the controller and third parties to whom the controller is responsible. There may, of course, be situations in which the processor has a legitimate interest in passing on data, e.g., when the processor needs to engage a subcontractor. However, because paragraph (2)(c) is only a default term, the processor and controller are free to agree on appropriate conditions for the engagement and duties of a subcontractor.

Illustration:

70. In the situation described in Illustration no. 69, P may require the services of an independent company to produce the digital twins. If this is the case, P must raise this point in the negotiations with C. P would need to procure C's agreement to use the independent company as a subcontractor. C and P might agree, for example, that the subcontractor is allowed so long as the same level of protection is ensured, plus that P remains fully responsible for what the subcontractor does.

Paragraph (2)(d) provides that the processor must refrain from any processing of the data for the processor's own purposes. This should not be interpreted as implying that the experience gained by the processor cannot benefit the processor in subsequent contracts. For instance, if the processor, in the course of fulfilling its duties under the contract for processing with the controller, uses artificial intelligence (AI), and that AI improves by being run on the controller's data, the processor may of course keep the improved AI and may benefit from that when dealing with the next customer. As this is merely an incidental effect of fulfilling the contract with the controller and does not harm the controller's interests, it is not prohibited by the default term under paragraph (2)(d). This is why paragraph (2)(d) contains an exception for when use of the data is reasonably necessary to improve the quality or efficiency of the relevant service, so long as this does not harm the controller's legitimate interests and is not inconsistent with any of the controller's legal obligations for the protection of third parties that could reasonably be expected in a situation of the relevant kind or of which the processor had notice when the contract was made.

Illustration:

71. Assume that P in Illustration no. 66 wants to process the data produced for C in two additional ways on which the contract document is silent: (a) analyzing it immediately for internal quality control and optimization of drone trajectories while the contract is still being performed, using only data that has been aggregated with data of other controllers, rendering it unattributable to the controller; and (b) retaining the data in a form that is still attributable to C to promote P's services. Use of the data in the first way is permitted by this default term because it is for the benefit of C and cannot harm C's interests, while use of the data in the second way would not be permitted by this default term because it is inconsistent with C's legitimate interest.

Paragraph (2)(e) addresses situations that may differentiate a contract for the processing of data from other service contracts. While a service provider who undertakes to apply fresh paint to a house, or to repair a car, or to transport goods from one place to another, has little opportunity to retain the materials provided by the other party after the contract has been performed, the situation is different with respect to data. In a contract for the processing of data, the processor would easily be able to retain a copy of the data without the controller's knowledge and at low cost for storage, etc., creating a temptation to use the data for a separate commercial purpose of the processor. Accordingly, paragraph (2)(e) supplies a default term of the contract to the effect that the processor must erase any data retained by the processor after the contract has been performed and the processed data has been provided to the controller. There may be some circumstances, however, in which retention of a copy of the data for a short period of time after the contract has been performed is not improper and is justified, e.g., by the processor's interest in defending itself in pending or imminent litigation. Even in those circumstances, however, retention of a copy would be a breach of the supplier's obligation if the terms of the contract indicate that retention of a copy is not allowed for that purpose (subject to rules of law that cannot be derogated from by agreement, such as doctrines of unconscionability).

Illustration:

72. Company P in Illustration no. 66 retains the data on its servers after having finished its service for C. Retaining the controller's data is normally not in conformity with the terms of the contract. However, if C has already announced it will withhold payment because the photographic material was not in conformity with the contract, P may have a legitimate interest in retaining the material in order to use it in potential litigation.

Under law governing the litigation process, a party may have a duty to preserve copies, in which case such a mandatory rule would govern.

c. Protection of third parties. Note that, not only does this Principle provide terms of the contract between the controller and the processor that relate to the protection of third parties, but in addition, Part IV provides rights directly to those third parties.

d. Rules applicable to contracts for processing of data. A contract for the processing of data under this Principle is a service contract. Legal systems typically do not differentiate between services in the brick-and-mortar world and services with regard to data. This is why paragraph (3) limits itself to stating that, in determining which rules and principles to apply directly or by way of

analogy, as provided in Principle 5, to contracts for processing of data, consideration should be given to the nature of the service, such as to whether the focus is on changing the data or on keeping it safe.

REPORTERS' NOTES

United States:

In the United States, a contract for the processing of data is governed by the general law of contracts (see generally Restatement of the Law Second, Contracts (AM. L. INST. 1981)). As is the case with all contracts, courts may supply contractual terms to address matters not addressed by the parties. See Restatement of the Law Second, Contracts § 5, Comment *b* (AM. L. INST. 1981) ("Much contract law consists of rules which may be varied by agreement of the parties. Such rules are sometimes stated in terms of presumed intention, and they may be thought of as implied terms of an agreement."). Restatement of the Law Second, Contracts § 204 further provides: "When the parties to a bargain sufficiently defined to be a contract have not agreed with respect to a term which is essential to a determination of their rights and duties, a term which is reasonable in the circumstances is supplied by the court." Id. § 204. Thus, paragraph (2) of this Principle can be seen as an enumeration of reasonable terms to be applied to the issues addressed in the absence of agreement of the parties.

Europe:

a. Scope and *b. Default terms applicable to contracts for processing of data.* The most important source for data processing contracts in Europe is Articles 28 ff of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) on the processing of personal data on behalf of a controller. Although those provisions are strongly influenced by the data protection context, they also include more general considerations of data governance in controller–processor relationships and of contractual means to achieve that governance. Therefore, they could be used as a model for data processing contracts under this Principle. Additional sources supporting the default terms in this Principle can be found in the Standard Contractual Clauses (SCC) for the transfer of personal data to third countries (Commission Implementing Decision (EU) 2021/914). The default terms in this Principle also have similarities to the default rules for service contracts under existing law. However, most of those existing rules are tailored to rivalrous assets and thus do not fully take into account the special characteristics of data, which is why these Principles partly deviate from those general rules.

Article 28(3)(a) of the GDPR obligates the processor to process the personal data only upon documented instructions from the controller, which is similar to the default rules in paragraph (2)(a) of this Principle. Clause 8 Module Two 8.1(a) of the SCC also sets out that the importer (i.e., processor) agrees and warrants to process the personal data only on documented instructions from the data exporter. Under a "traditional" service contract, the service provider is—similar to paragraph (2)(a) of this Principle—generally obligated to follow directions of the client regarding the performance of the service. However, those directions must be timely, and be part of the

contract itself, or specified in a document to which the contract refers; result from the realization of choices left to the client by the contract; or result from the realization of choices initially left open by the parties (see Article IV.C. – 2:107(1) Draft Common Frame of Reference (DCFR)). If the direction bears the risk that the result stated or envisaged by the client will not be achieved, or may damage other interests of the client, the service provider must warn the client (Article IV.C. – 2:107(2) and Article IV.C. – 2:108(1) DCFR).

An obligation comparable to paragraph (2)(b) of this Principle can be found in Article 28(1) of the GDPR, which requires the controller to only use processors who provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the data subject's rights. There is also a resemblance between Clause 8 Module Two 8.6(a) of the SCC and paragraph (2)(b) of this Principle. Pursuant to Clause 8 Module Two 8.6(a), the importer shall implement appropriate technical and organizational security measures to ensure the security of the data. Further, the duties in the default terms in paragraph (2) draw clear inspiration from the duties of a storer in a storage contract, which is a special form of a service contract, under which the storer is obligated to take reasonable precautions in order to prevent unnecessary deterioration, decay, or depreciation of the object stored (Article IV.C. – 5:103(1) DCFR). In addition, the storer may use the object entrusted for storage only if the client has agreed to such use (Article IV.C. – 5:103(2) DCFR).

Article 28(3)(g) of the GDPR stipulates that the processor shall delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data, which corresponds to paragraph (2)(e) of this Principle (as well as to Principle 15(2)(c)). Similar provisions can be found in other parts of the GDPR, e.g., in Article 17 of the GDPR on erasure of the data and also in Article 16(3) of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770), according to which, upon termination of the contract, the trader shall generally refrain from further use of content provided by the consumer under the contract. Also, under Clause 16(d) of the SCC, the data that has been transferred prior to the termination of the contract shall immediately be returned to the data exporter or deleted in its entirety; the same shall apply to any copies of the data. Similarly, a storer in a storage contract must return the object at the agreed time or, if the contractual relationship is terminated before the agreed time, within a reasonable time after being so requested by the client (Article IV.C. – 5:104(1) DCFR), which is also set out for the data resulting from the processing that has not already been transferred in paragraph (2)(e) of this Principle.

d. Rules applicable to contracts for processing of data. Under national legal systems, data processing contracts are normally categorized as contracts for service. At their core, service contracts are understood as the supply of a service in exchange for remuneration. However, there are differences in European legal systems as to the exact definition of service contracts. Some jurisdictions have different rules for material and intellectual services, while others apply the same provision for all services other than storage. While all legal systems in the European Union have specific rules on storage contracts, their application usually requires that a tangible good be stored. Thus, in most legal systems, the provisions for contracts for service also apply to cloud storage

contracts. An exception is Germany, where cloud computing contracts are generally classified as lease/rental agreements that may have certain elements of a service contract.

In English law, contracts for services are defined very broadly as "any contract under which a person agrees to carry out a service" in Section 12(1) of the Supply of Goods and Services Act 1982. The range of activities covered by that definition is very wide and covers both material and intellectual services. Explicitly excluded from that statutory definition are contracts of service (employment contracts) and contracts of apprenticeship. According to Section 12(3) of that Act, a contract does not fall outside the definition of a "contract for services" merely because goods are transferred or bailed by way of hire. That broad definition is likely to cover most data processing contracts.

In France, the concept of "louage d'ouvrage" (also: contrat de prestation de service) is very broad in the sense that it covers any contract whereby one party agrees to perform work for another party on an independent basis. The contract does not only include services relating to immovable and movable objects but, according to a decision of the French Cour de Cassation, also covers intellectual services (Cass. Civ. III, 28 February 1984, Bull. civ. III, no. 51). Therefore, the general provisions on louage d'ouvrage (cf. Articles 1710, 1779 and 1787 ff. French Code Civil) also apply to the contracts referred to by this Principle.

The German Civil Code distinguishes between "Werkvertrag" (when the service provider undertakes to achieve a particular result) and "Dienstvertrag" (when the service provider only promises best efforts). The concept of Werkvertrag, which is laid down in Sections 631 ff., is considered to cover all kind of services, and applies to services related to immovables and movables, but also to intellectual services (cf. Section 631 (1)) and is thus also likely to cover most data processing contracts. However, Dienstvertrag (Sections 611 ff) may also cover a wide range of different types of data processing services that would be covered by this Principle. Some services covered by this Principle, such as contracts for the storage of data in a cloud, would be classified in a different manner, e.g., as lease (rental) contracts (Sections 535 ff., 578b).

Principle 13. Data Trust Contracts

(1) A data trust contract is a contract among one or more controllers of data (the "entrusters") and a third party under which the entrusters empower the third party (the "data trustee") to make certain decisions about use or onward supply of data (the "entrusted data") on their behalf, in the furtherance of stated purposes that may benefit the entrusters or a wider group of stakeholders (such entrusters or stakeholders being referred to as the "beneficiaries").

(2) A data trust contract and the relationships it creates need not conform to any particular organizational structure and need not include the characteristics and duties associated with a common law trust. This Principle applies, with appropriate adjustments, to the governing principles of any entity created pursuant to a data trust contract.

(3) Subject to agreement of the parties and to rules that take priority under Principle 5, the law should provide that the following terms are included in a data trust contract or are incorporated into the governing principles of any entity created pursuant to the data trust contract:

(a) the data trustee is, subject to paragraphs (3)(b) and (3)(c), empowered to make and implement all decisions with regard to use or onward supply of the entrusted data, including decisions concerning intellectual property rights and rights based on data privacy/data protection law;

(b) the data trustee must act in furtherance of the stated purposes of the data trust contract for the benefit of the beneficiaries and, even if the entrusters are not the beneficiaries, in a manner that is not inconsistent with the legitimate interests of the entrusters of which the data trustee has notice;

(c) the data trustee must follow any directions given by the entrusters, including by allowing the porting of data at the entrusters' request at any time, except to the extent that the data trustee has notice that the directions are incompatible with the stated or manifestly obvious purposes of the data trust;

(d) the data trustee must refrain from any use of the entrusted data for its own purposes and must avoid any conflict of interest;

(e) the entrusters may terminate the data trustee's power with regard to the data entrusted by them at any time; however, this right may be limited to the extent necessary to take into account reliance and similar legitimate interests of the beneficiaries; and

(f) if the data trustee has retained any data entrusted, or any data derived from such data, after the contract has come to an end (by termination or otherwise) the data trustee must return the data to the entrusters, and, when reasonable, take steps to prevent further use of the data by onward recipients.

(4) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to data trust contracts, consideration should be given in particular to:

(a) the stated purposes of the data trust contract and the nature of the data and of the parties involved;

(b) whether the purposes of the data trust contract are primarily for the benefit of the entrusters or broader constituencies; and

(c) the organizational structure of the relationships created by the data trust contract.

Comment:

a. Scope. This Principle provides a general overview of the legal principles recommended for data trust contracts. As noted in paragraph (2), notwithstanding the use of the term "trust" in the nomenclature describing these arrangements, the arrangements need not include the characteristics and duties associated with a common law trust. This Principle is stated at a high level of generality because both the subject of data trust arrangements and the nature of those arrangements can vary widely. Moreover, data trust arrangements are an emerging concept, with new subjects and mechanisms constantly arising. The purpose of this Principle, as of most other Principles, is facilitative. Thus, the description of types of data trust contracts, and the recommended rules to govern them, are not limited to arrangements that are common today; rather, they are designed to be flexible enough to accommodate arrangements that may emerge in the future.

Data trust arrangements within the meaning of this Principle are often combined with arrangements for the processing of data within the meaning of Principle 12, as the data trustee's activities under the data trust arrangements would often include storage of data and similar data processing activities. When this is the case, both Principle 12 and this Principle would apply, with this Principle more specifically dealing with the power of decisionmaking, i.e., a power that rests with the controller of data, and not with the processor. A data trustee is thus a person to whom one or more controllers of data delegate (some of) their powers as controllers, while possibly engaging the same party to provide other services under Principle 12.

Data trust arrangements are typically contracts that create a continuing relationship of a particular or indefinite duration. While, theoretically, any contract dealt with under these Principles could be either a one-time exchange or a continuing relationship, the contracts dealt with under this Principle, as well as some other Principles, are more often entered into for a particular or indefinite period of time.

b. Typical data trust arrangements. Under this Principle, a wide variety of arrangements may be governed as data trust contracts. All that is needed is a contract of the sort described in paragraph (1) among an entruster or entrusters and a data trustee under which the data trustee is empowered and directed to make decisions about use and onward supply of the data in furtherance

of the stated purpose. Despite this generality, and the wide-open possibilities that it suggests, some types of data trust contracts that are found at present can be identified and described.

For example, one common type of data trust contract (as that term is used in this Principle) is a data management contract, under which one party undertakes to manage data on behalf of another party. An example is provided by personal information management services (PIMS), also known as personal data stores, personal data spaces, or personal data vaults, under which the party undertaking to manage the data (the "data trustee" under the nomenclature of this Principle) is empowered to make decisions on behalf of the entruster with respect to intellectual property issues, data protection, etc. Such arrangements involve a requirement that the data trustee manage the data for the interest of the entrusters and follow directions that they may give, subject to the entruster's right to withdraw from the arrangement at any time. In some ways, such an arrangement is akin to an agency arrangement, with the entruster as principal and the data trustee as agent.

Illustration:

73. Several individuals contract with a service provider M under an arrangement in which these individuals provide to M access to certain personal information collected by and stored on their respective mobile devices. M is given the power to interact with website operators that seek personal information from visitors to their websites and disclose only such information under such conditions as meets criteria established in the contract. The contract is a data trust contract.

Another common type of data trust arrangement is an arrangement under which one party (the data trustee) undertakes to control data it has been entrusted with for a stated purpose, e.g., data donation for health research. As with the data management contract, the greater expertise of the data trustee is a motivating factor in entering into the arrangement.

Illustration:

74. A large number of health care providers contract with data trustee T to provide to T access to data about cases of certain infectious diseases so that T can manage the data and make it available under specified terms to inform disease-control programs in order to target interventions and improve health service coverage. This contract is a data trust contract.

c. *Structure.* The arrangement created by a data trust contract can take many forms. In some cases, the data trust contract may result in the formation of a common law trust (in jurisdictions where that concept exists), but this is not necessary. Similarly, the data trust contract may result in the creation of other arrangements that use trust nomenclature even though they are not common law trusts, such as a Massachusetts Business Trust or a Delaware Statutory Trust or Purpose Trust, but this is not necessary either. Rather, the distinguishing feature of the data trust contract is the agreement pursuant to which decisions about access to and use of data are to be made collectively in furtherance of the stated purposes and for the benefit of the beneficiaries. The form of such an agreement, and the decisionmaking structure that results from it, is not constrained by these Principles; of course, other law, such as competition law and data privacy/data protection law, may apply and, in some cases, place limits.

d. Distinguishing between the data trust contract and legal structures it may create. It is important to distinguish the data trust contract—the contract among the entrusters and the data trustee under which the governing structure is created—from law governing the structure itself. For example, if the agreement calls for the formation of a common law trust, with a trustee holding the data for the benefit of beneficiaries to whom the trustee owes a fiduciary duty, the law applicable to such common law trusts applies. Similarly, if the data trust contract calls for the formation of a typical for-profit corporation or a public benefit corporation, the law governing such corporations governs their internal affairs. It should be noted, however, that the law governing structures that may be created by a data trust contract often provides for a substantial role for private ordering by agreement among stakeholders. Examples include shareholder agreements with respect to a corporation and the terms of the trust instrument in the case of a trust. The data trust contract can be seen, therefore, not only as the agreement to create a particular structure but also as an agreement among the stakeholders in the context of that structure.

Thus, while the default terms provided by this Principle do not impose fiduciary duties in data trust arrangements, the form or structure selected by the parties to effectuate their data trust arrangement may do so. In such cases, the fiduciary duties are those created by the law governing the form or structure, and those duties augment the duties imposed by this Principle.

e. Default terms. The default terms for a data trust contract as described in this Principle are necessarily general in light of the variety of situations in which such a contract may be utilized and the variety of arrangements that the parties may devise.

First, paragraph (3)(a) provides a term relating to the power to make decisions with regard to use and onward supply of the entrusted data. Under this term, the data trustee is, by default, given the power to make all types of decisions with regard to the data, i.e., in the event of doubt the power vested in the trustee is broader rather than narrower. However, that power is always subject to paragraphs (3)(b) and (3)(c), i.e., to the furtherance of the stated purpose of the data trust contract and the benefit of the beneficiaries and the legitimate interests of the entrusters, as well as to any specific directions given by the entrusters.

Illustration:

75. Assume that in a scenario such as the one in Illustration no. 74 the agreement between the health care providers and trustee T does not specify clearly which kind of decisions T may take with regard to the data, i.e., it is unclear whether T may pass the data on only to public bodies or may also sell the data to private companies. Under paragraph (3)(a) of this Principle the trustee may make such decisions, subject to paragraphs (3)(b) and (3)(c).

Second, paragraph (3)(b) provides that the data trustee's primary obligation is to act in furtherance of the stated purposes of the data trust contract for the benefit of the beneficiaries. This is a critical point inasmuch as it means that gaps or incompleteness in the data trust contract will be filled with terms that are primarily guided by the purpose of the contract (which may differ from the private interests of the parties).

Third, paragraph (3)(c) provides a default rule directing the data trustee to follow directions given by the entrusters. In line with Principle 12(2)(a), this may also include the porting of the data at the entrusters' request at any time. This rule has an important limit, however; the trustee need not (or even must not) follow directions when the trustee could reasonably be expected to realize that the directions are incompatible with the stated purposes of the data trust. Thus, unless otherwise agreed, the stated purposes of the trust serve as an outside limit on the power of entrusters to direct the data trustee.

Illustration:

76. If T in Illustration no. 75, by selling the data to private companies, would be jeopardizing the legitimate interests of the health care providers, e.g., by potentially disclosing very sensitive data about the patients treated by those health care providers and

putting the health care providers at risk of being sued by their patients for breach of confidentiality, the power vested in T does not include the power to sell the data to the private companies as this would be incompatible with paragraph (3)(b) of this Principle. The health care providers could, in addition, give binding directions to T under paragraph (3)(c) to refrain from selling the data. However, they could not give directions to T to sell the data if this is in violation of the stated purposes of the data trust contract (e.g., if that stated or manifestly obvious purpose includes protection of patients' rights).

Fourth, paragraph (3)(d) provides a default rule that protects entrusters from data trustees who might use their position to benefit themselves rather than the entrusters. This rule prohibits the trustee from using the data to serve its own ends rather than the purposes of the entrusters; more generally, this rule directs data trustees to avoid conflicts of interest with respect to the data and its stewardship. This is so irrespective of whether the use of the data would also be in violation of the default term under paragraph (3)(b) of this Principle.

Illustration:

77. If T in Illustration no. 75 decided to form a research company and use the data it has been entrusted with for that company's own research, T would be violating the default term under paragraph (3)(d) of this Principle.

Fifth, paragraph (3)(e) addresses the ability of the entrusters to terminate the powers of the data trustee. The term proposed enables the entrusters to terminate the powers of the data trustee at any time (much like termination without cause in the corporate context). This right, however, is limited to the extent necessary to take into account legitimate interests of the beneficiaries of the data trust.

Finally, paragraph (3)(f) states that, upon termination, the data trustee must return any entrusted data the trustee has retained, or any data derived from such data, and, when reasonable, take steps to prevent further use of the data by any onward recipients. This provision is similar to that of Principle 12(2)(e) and if the data trustee may also be considered a processor under Principle 12 (which may or may not be the case), the obligation to erase might follow from both Principles.

Illustration:

78. If in Illustration no. 71, one of the health care providers entrusting T with its data, decides that it no longer wishes to participate in the arrangement, it may, under

paragraph (3)(e) of this Principle, terminate the arrangement with T at any time. This would mean T may no longer make any decisions with regard to that health care provider's data. If that health care provider had transferred the data to storage space within T's control, T would have to erase that data. If T has passed the data on to others, the question whether T must also take steps to prevent further use of the data by those onward recipients depends on whether that is reasonable. What counts as "reasonable" depends on many factors, including applicable law (such as data protection/data privacy law), any potential adverse effects on the entrusters, and the terms of the contractual arrangements T has entered into with the onward recipients in fulfilment of its duties as data trustee.

f. Incorporation of default terms into governing principles of structure of the data trust. In light of the fact that, as noted in Comment *d*, a data trust contract often calls for the creation of a structure, such as a corporation or common law trust, that has its own governance principles that allow for the autonomy of the parties to shape their relationship, paragraph (3) also provides that the default terms may be effectuated by being incorporated into the governing principles of an entity created pursuant to the data trust contract rather than into the data trust contract itself.

g. Analogies. As noted in paragraph (4), this Principle suggests three approaches to identifying analogies as the source of rules to govern data trust contracts. The first, consistent with principles involving arrangements of entrustment in general, is to take into account the stated purposes of the contract as well as the nature of the data and the parties involved. Second, the appropriate analogy will depend on whether the purposes of the data trust contract are primarily for the benefit of the entrusters or broader constituencies. Law has long taken different approaches to arrangements that are primarily for private benefit and those that are primarily for public benefit. Thus, if the purpose of the data trust contract is public benefit, appropriate analogies should be drawn. Third, the nature of any organizational structure created by the data trust contract can supply analogies. For example, if the data trust contract contemplates the creation of a corporation that will manage and exploit the data on behalf of the entrusters, an analogy to shareholder agreements in corporations would be useful.

REPORTERS' NOTES

United States:

In the United States, a data trust contract would be governed by the general law of contracts (see generally Restatement of the Law Second, Contracts (AM. L. INST. 1981)). As is the case with

all contracts, courts may supply contractual terms to address matters not addressed by the parties. See id. § 5, Comment *b* ("Much contract law consists of rules which may be varied by agreement of the parties. Such rules are sometimes stated in terms of presumed intention, and they may be thought of as implied terms of an agreement."). Restatement of the Law Second, Contracts § 204 (AM. L. INST. 1981) further provides that "When the parties to a bargain sufficiently defined to be a contract have not agreed with respect to a term which is essential to a determination of their rights and duties, a term which is reasonable in the circumstances is supplied by the court." Thus, paragraph (3) of this Principle can be seen as an enumeration of reasonable terms to be applied to the issues addressed in the absence of agreement of the parties.

As to common law trusts, see generally Restatement of the Law Third, Trusts (AM. L. INST. 2003, 2007, 2012). In particular, see § 2 of that Restatement for a definition of the term "trust" and § 5 for an enumeration of relationships that do not constitute trusts.

As for the nature of Massachusetts Business Trusts, see, e.g., Comment, *The Nature of Massachusetts Business Trusts*, 27 YALE L.J. 677 (1918). With respect to statutory trusts, see, e.g., DEL. CODE ANN. tit. 12, § 3801 et seq. For a data trust arrangement as to which there are no beneficiaries that are distinct from the entrusters, one possible entity is the so-called "purpose trust." See, e.g., S.D. CODIFIED LAWS §§ 55-1-20 et seq. For a hybrid version with some beneficiaries, some U.S. states have created "hybrid purpose trusts." See, e.g., S.D. CODIFIED LAWS § 55-1-22.

Illustrations 74 to 78 are based on DiSARM (Disease Surveillance and Risk Monitoring project). See https://www.disarm.io/.

Europe:

a. Scope and *b. Typical data trust arrangements.* In Europe, the term "data trust" has been on everyone's lips for quite some time, and these arrangements are often seen as a panacea for a range of different problems in the data economy. One form of data trusts are personal information management systems (PIMS), which are also supported by the European Commission in its data strategy for Europe (cf. COM(2020) 66 final, p. 10), the German Data Ethics Commission (Opinion of the German Data Ethics Commission, 2019, p. 133 ff.) and the Data Strategy of the German Federal Government (Datenstrategie der Bundesregierung, 2021, p. 33 ff). While mere privacy management tools (PMT) support data subjects in managing their personal data, PIMS support data subjects with exercising some of the data subject's rights under data protection law, such as withdrawal of consent or porting requests. The concept of "data trusteeship" (cf. Christiane Wendehorst, Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy, in Sebastian Lohsse, Rainer Schulze and Dirk Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, p. 327, 346 et seq.) is somewhat broader, as it includes not only sophisticated PIMS, vested with a mandate to exercise data rights on behalf of the data subject according to standardized directions and preferences, but also the management of intellectual property rights, like copyright in user-generated content, or the management of non-personal data.

Chapter III of the Data Governance Act (DGA) (Regulation (EU) 2022/868) contains rules on "data intermediation services" (Articles 10 ff). The DGA covers three types of services in its

Article 10. The first type is intermediation services between data holders and potential data users, including making available the technical or other means to enable such services—those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users. The second type of service is intermediation services between data subjects that seek to make their personal data available and potential data users, including making available the technical or other means to enable such services, in the exercise of the rights provided in the General Data Protection Regulation (GDPR). Finally, the third type of service is services of data cooperatives, that is to say services supporting data subjects or one-person companies or micro-, small-, and medium-sized enterprises (MSMEs), who are members of the cooperative or who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent, in making informed choices before consenting to data processing, and allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons.

The first of these three types of data intermediation services would be classified as a data marketplace contract under Principle 15. However, the types addressed by Article 10(b) and 10(c) of the DGA would be data trust contracts within the meaning of this Principle. The DGA is unclear as to whether a data subject can delegate or even assign the exercise of the data subject's rights to a data intermediation service provider. Arguably, this is possible only to a very limited extent (Recital 31 DGA).

d. Distinguishing between the data trust contract and legal structures it may create. In Europe, different models as to ownership structure can be envisaged. The choice between those models can be determined by the need to ensure that the interests of the trustee are aligned with those of the individuals it represents (see Aline Blankertz, Designing Data Trust, 2020, p. 24). The main options discussed are the following: (a) a private, for-profit company that is sufficiently independent from any other business in the data economy, which may imply restrictions on who may own how many shares; (b) a not-for-profit collecting society of the kind found in the area of copyright law; (c) a state authority.

The Data Governance Act avoids conflicts of interests by setting out that these intermediaries have to separate their data intermediation services from other services (Recital 33 DGA). That means that the data intermediation service should be provided through a legal person that is separate from the other activities of the provider (Article 12(a) DGA). In addition, those intermediaries should bear fiduciary duties toward the individuals, to ensure that they act in the best interests of the data holders (Recital 33 DGA).

e. Default terms and *g. Analogies.* According to the definition in this Principle, a "data trust contract" would often be classified as a "trust" or a "mandate" in Europe. A trust is typically defined as a "legal relationship in which a trustee is obliged to administer or dispose of one or more assets in accordance with the terms governing the relationship to benefit a beneficiary or advance public benefit purposes" (see Article X. – 1:201 Draft Common Frame of Reference (DCFR)). A mandate is a contract under which "a person, the agent, is authorized and instructed (mandated) by another person, the principal, (a) to conclude a contract between the principal and a third party or otherwise directly affect the legal position of the principal in relation to a third party; (b) to

conclude a contract with a third party, or do another juridical act in relation to a third party, on behalf of the principal but in such a way that the agent and not the principal is a party to the contract or other juridical act; or (c) to take steps which are meant to lead to, or facilitate, the conclusion of a contract between the principal and a third party or the doing of another juridical act which would affect the legal position of the principal in relation to a third party" (Article IV.D. – 1:101 DCFR).

In Europe, trustees are typically entitled to do any act in performance of the obligation under the trust (see Article X. – 5:201 DCFR; Article V(1) of the Principles of European Trust Law), which is also set out in paragraph (3)(a) of this Principle. However, the powers of the trustee are typically limited by restrictions in the trust terms and to such acts that an owner might lawfully do or a person might be authorized to do on behalf of another (Article X. – 5:201 DCFR).

A trustee is generally obligated to exercise any power for the benefit of the beneficiaries or the advancement of public benefit purposes, in accordance with the law and the trust terms (Article X. – 6:101 DCFR; Article 5(2) European Principles of Trust Law). This is also set out as a default term for data trustees in paragraph (3)(b) of this Principle; however, if the entrusters are not the beneficiaries, the trustee may act in a manner that is not inconsistent with the legitimate interests of the entrusters of which the data trustee has notice. Such an obligation can also be found in mandate contracts under which the agent must act in accordance with the interests of the principal, insofar as these have been communicated to the agent or the agent could reasonably be expected to be aware of them (Article IV.D. – 3:102 DCFR).

The trust terms or the public benefit purpose typically serve as an outside limit of the trust, as is stated in paragraph (3)(c) of this Principle. Therefore, a trustee is in breach of his or her contractual duty if the trustee exercises powers that are not in accordance with the law or the trust terms (Article X. – 6:101 DCFR; Article 5(2) of the European Principles of Trust Law). The duty to follow the directions of the entruster is similar to directions under mandate contracts. An agent must generally follow any direction by the principal (Article IV.D. – 4:101(2) DCFR). However, if the direction is inconsistent with the purpose of the mandate contract or may otherwise be detrimental to the interest of the principal, the agent has to warn the principal (Article IV.D. – 4:101(2)(b) DCFR). If the principal does not revoke the direction without undue delay after having been warned, the mandate is changed to the direction (Article IV.D. – 4:201(1)(b) DCFR). The default rule is also similar to the obligation in mandate contracts under which the agent must act in accordance with the interests of the principal, insofar as those have been communicated to the agent or the agent could reasonably be expected to be aware of them (Article IV.D. – 3:102 DCFR).

Paragraph (3)(d) of this Principle ensures the neutrality of the data trust by prohibiting the use of the data for the data trustee's own purposes. This restriction can also be found in the DGA, which stipulates that the provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users (Article 12(a) DGA). The same holds true for the data collected with respect to any activity of a natural or legal person for the purposes of the provision of the data intermediation service, which may only be used for the development of that service (Article 12(c) DGA). The provider shall also act in the data subjects' best interests when facilitating the exercise of their rights (Article 12(m) DGA). A similar duty can also be found with regard to trusts; the trustee is obligated not to make use of the fund, or information or an

opportunity obtained in the capacity of trustee, to obtain an enrichment unless authorized by the trust terms (Article X. – 6:109 DCFR).

The right to terminate a data trust at any time (paragraph (3)(e) of this Principle) is identical to the right to terminate a mandate contract (Article IV.D. – 6:101 DCFR); revocation of the mandate of the agent is also treated as termination of the mandate contract (Article IV.D. – 6:101 DCFR). However, the right to terminate contracts can also be restricted as with trusts when the right to terminate is generally available for a beneficiary of the trust to the extent that it is for the beneficiary's exclusive benefit (see Article X. – 9:104 DCFR), but an entruster that is not a beneficiary is only entitled to terminate the trust to the same extent that he or she might have revoked a donation to the beneficiary if the benefit had been conferred by way of donation (Article X. – 9:103 DCFR).

The last default rule (paragraph (3)(f) of this Principle) corresponds to Article 28(3)(g) of the GDPR, which stipulates that the processor shall delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data. Furthermore, Article 16(3) of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) provides that, upon termination of the contract, the trader shall refrain from further use of content provided by the consumer under the contract.

Principle 14. Data Escrow Contracts

(1) A data escrow contract is a contract among one or more parties planning to use data (the "contracting parties") and a third party (the "escrowee") under which the escrowee undertakes to make sure the powers and abilities of some or all of the contracting parties with respect to the data are restricted (the "restricted parties") so as to avoid conflict with legal requirements, such as those imposed by antitrust law or data privacy/data protection law.

(2) A data escrow contract and the relationships it creates need not conform to any particular organizational structure. This Principle applies, with appropriate adjustments, to the governing principles of any entity created pursuant to a data escrow contract.

(3) Subject to agreement of the parties and to other principles that take priority under Principle 5, the law should provide that the following terms are included in a data escrow contract or are incorporated into the governing principles of any entity created pursuant to the data escrow contract:

(a) the escrowee has such powers with regard to the data as are necessary for the stated purpose of the data escrow contract;

(b) the escrowee must act in furtherance of the stated purposes of the data escrow contract even if such action is inconsistent with interests of the contracting parties that are distinct from the stated purpose of the data escrow contract;

(c) the escrowee must not follow any direction given by a contracting party that is incompatible with the stated or manifestly obvious purpose of the data escrow contract;

(d) the escrowee must refrain from any use or onward supply of the entrusted data for its own purposes and must avoid any conflict of interest; and

(e) if the data escrow contract is terminated, each party has an obligation during the winding-up of the relationship not to take actions that undermine the stated purposes of the data escrow contract.

(4) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to data escrow contracts, consideration should be given in particular to:

(a) the stated purpose of the data escrow contract and the nature of the data and of the parties involved; and

(b) the organizational structure of the relationships created by the data escrow contract.

Comment:

a. Scope. This Principle provides a general overview of the legal principles recommended for data escrow contracts. It is stated at a high level of generality because, as with data trust contracts, both the subject of data escrow contracts and their nature can vary widely, and data escrow contracts are still an emerging concept. The main difference between a data escrow contract under this Principle and a data trust contract under Principle 13 is that the purpose of a data escrow contract is to limit the powers of some or all parties contracting with the escrowee, whereas under a data trust contract the trustee must, at the end of the day, follow the directions and defer to the powers of the entrusters. This difference entails several consequences, resulting in a set of default terms that is distinct from that under Principle 13.

b. Purposes of data escrow arrangements. The essence of a data escrow contract is that the restricted parties either divest themselves of (full) control of data they hold, transferring that control to a third party (the escrowee), or take steps to ensure they will never get (full) control of particular data. It might seem anomalous for a party to voluntarily surrender or renounce control. There are,

however, situations in which, for regulatory reasons or the like, it is important for a person with rights or powers with respect to data to surrender or renounce control of that data. Antitrust considerations (and related demands of competition law) are one example of such a situation; another example is provided by data privacy and data protection law. In such cases, the parties can avoid running afoul of important legal rules by renouncing control of data that they would otherwise have.

Illustration:

79. European company C would like to use a customer management system, run by U.S. software company S. In order to comply with European data protection law, C must ensure its customers' personal data are not transferred to the United States unless there are sufficient guarantees in place that ensure U.S. authorities cannot access the data merely upon a request made to S. In order to be able to make the deal, C and S therefore enter into an agreement with trusted third party E, according to which customer data will be transferred to S only in encrypted form, and it will be only with the help of keys held by E that it will be possible to decrypt the customer data. The arrangement between S and E is a data escrow contract.

c. *Structure.* The arrangement created by a data escrow contract can take many forms. In some cases, especially in legal systems in which escrow arrangements are common and well understood, the arrangement may be created by an agreement that spells out the terms of the escrow arrangement. In other cases, however, the data escrow contract may provide for the formation of an entity of sorts to hold the escrowed data. It is important to distinguish the data escrow contract—the contract among the contracting parties and the escrowee under which the governing structure is created—from law governing the structure itself. For example, if the agreement calls for the formation of a public benefit corporation, the law governing such corporations governs its internal affairs. It should be noted, however, that the law governing structures that may be created by a data escrow contract often provides for a substantial role for private ordering by agreement among stakeholders. Examples include shareholder agreements with respect to a corporation and the terms of the trust instrument in the case of a trust. The data escrow contract can be seen, therefore, not only as the agreement to create a particular structure but also as an agreement among the stakeholders in the context of that structure.

d. Default terms. The default terms for a data escrow contract as described in this Principle are necessarily general in light of the variety of situations in which such a contract may be utilized and the variety of arrangements that the parties may devise. Accordingly, paragraph (3) identifies only a small number of default terms, which are applicable to all of these arrangements in case the contract is silent, and leaves it to the parties to adapt the arrangement to their relevant data escrow model in detail.

First, paragraph (3)(a) provides the key governing principle—the escrowee has whatever powers are necessary for accomplishment of the stated purposes of the data escrow contract.

Second, paragraph (3)(b) provides that the escrowee's primary obligation is to act in furtherance of the stated or manifestly obvious purposes of the data escrow contract. This is a critical point inasmuch as it means that gaps or incompleteness in the data trust contract will be filled with terms that are primarily guided by the purpose of the contract (which may differ from the private interests of the parties). Moreover, paragraph (3)(b) provides that the escrowee has this obligation even if its actions would be inconsistent with interests of the contracting parties that are distinct from the stated purpose of the data escrow contract.

It follows from this rule that paragraph (3)(c) provides that the escrowee must not follow directions from contracting parties when the directions are inconsistent with the stated or manifestly obvious purpose of the arrangement.

Illustration:

80. S and E in Illustration no. 79 did not agree on the exact conditions under which S may, as far as necessary for software maintenance, get access to particular sample datasets. This gap is to be closed by reference to the purpose of the data escrow contract, which is compliance with European data protection law. So, E must take whatever steps are needed to ensure that the requirements of European data protection law are fulfilled. This is so even when S (or even both S and C) directs E to transfer particular datasets to the United States

Fourth, paragraph (3)(d) provides a default rule that protects contracting parties from escrowees who might use their position to benefit themselves rather than the position of the contracting parties. This rule prohibits the escrowee from using the data to serve its own ends rather than the purposes of the contracting parties.

Finally, paragraph (3)(e) provides that if the data escrow contract is terminated, the winding up of the relationship must not occur in a way that poses a threat to the stated purposes of the data escrow contract. In some circumstances, particularly when the purpose of the data escrow contract is to ensure that the restricted parties do not have (full) control of the data, this may mean that a substitute escrowee should succeed to the interest of the original escrowee, or that some other mechanism should be created to ensure that the purpose of the arrangement is not undermined, rather than having control revert to restricted parties.

Illustration:

81. If the contract with E in Illustration no. 79 is terminated, this does not mean that the data can simply be made accessible to S without encryption, because this granting of access would be in breach of the stated purpose. Instead, compliance with applicable data protection law would have to be ensured by other means.

e. Incorporation into governing principles of data escrow structure. In light of the fact that, as noted in Comment *c*, a data escrow contract often calls for the creation of a structure, such as a corporation or common law trust, that has its own governance principles that allow for the autonomy of the parties to shape their relationship, paragraph (3) also provides that the default terms of a data escrow contract may be effectuated by being incorporated into the governing principles of an entity created pursuant to the data escrow contract rather than into the data escrow contract itself.

f. Analogies. As noted in paragraph (4), this Principle suggests two approaches to identifying analogies as the source of rules to govern data escrow contracts. The first approach is to take into account the stated purpose of the data escrow contract and the nature of the data and of the parties involved. The focus on the stated purpose is particularly apt in light of the purposes for which data escrow arrangements are typically established, as described in Comment *b.* Second, the nature of any organizational structure created by the data escrow contract can supply analogies. For example, if the data escrow contract contemplates the creation of a corporation that will manage and exploit the data, an analogy to shareholder agreements or proxies in corporations would be useful.

REPORTERS' NOTES

United States:

In the United States, a data escrow contract would be governed by the general law of contracts (see generally Restatement of the Law Second, Contracts (AM. L. INST. 1981)), as applied in escrow contracts. As is the case with all contracts, courts may supply contractual terms to address matters not addressed by the parties. See id. § 5, Comment *b* ("Much contract law consists of rules which may be varied by agreement of the parties. Such rules are sometimes stated in terms of presumed intention, and they may be thought of as implied terms of an agreement."). Restatement of the Law Second, Contracts § 204 further provides that "When the parties to a bargain sufficiently defined to be a contract have not agreed with respect to a term which is essential to a determination of their rights and duties, a term which is reasonable in the circumstances is supplied by the court." Id. § 204. Thus, paragraph (3) of this Principle can be seen as an enumeration of reasonable terms to be applied to the issues addressed in the absence of agreement of the parties.

The term "escrow" is traditionally used in the United States to refer to situations in which the asset held by the escrowee is money. See, e.g., Howard v. Chi. Transit Auth., 931 N.E.2d 292, 297 (Ill. App. Ct. 2010) ("In an escrow contract, a grantor and a third party execute a written instrument under which the grantor gives funds to the third party to hold until a designated time when those funds are delivered to a grantee."). Thus, the usage in these Principles, in which the subject of the escrow is data, rather than money, is an adaptation of that standard usage. Similar adaptations have occurred in a variety of contexts, such as software source code escrow.

Europe:

a. Scope and *b. Purposes of data escrow arrangements.* Data escrow models are used in Europe to ensure legal compliance. One example is the storage of car accident data of connected vehicles. Section 63a para 1 of the German Road Traffic Act requires motor vehicles with a highly or fully automated driving function to store position and time information determined by a satellite navigation system if there is a change in vehicle control between the driver and the highly or fully automated system. The vehicle owner must arrange for the transmission of the relevant data to third parties if this is necessary for the assertion, satisfaction, or defense of legal claims. However, if the data is controlled by the manufacturer, the latter might seek to avoid possible claims against itself. To overcome this difficulty, the introduction of an intermediary has been proposed. The relationship among this intermediary, the manufacturer, and the car owner would qualify as a data escrow contract, because it would limit the manufacturer's powers as to the data.

Another example is data protection in the case of onward transfer after the Schrems II Judgment by the Court of Justice of the European Union (CJEU) (C-311/18 ECLI:EU:C:2020:559 – *Schrems II*), where data escrow contracts under this Principle could serve as such supplementary measures, which has also been highlighted by the European Data Protection Board (EDPB) in its Recommendation 01/2020 (EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 2020). The EDPB stated that strong encryption before transmission could provide an effective supplementary measure, if the keys are retained solely under the control of the exporters or other entities entrusted

with that task (EDPB, Recommendations 01/2020, p. 22 f.). Thus, data escrow contracts under this Principle could be a key element to ensure an equivalent level of protection of the personal data in onward transfers from the European Union to the United States.

Involving trusted third parties has also been intensively discussed as a matter to avoid Article 101(1) of the Treaty on the Functioning of the European Union (TFEU) infringements, especially when concluding data pooling contracts. Data sharing between competitors always has the potential to create anticompetitive effects due to the possible exclusion of non-participating competitors, including potential future competitors who have not yet entered the market. This is the case in which the data contains relevant strategic and competitive information, such as costs and prices (Björn Lundqvist, Competition and Data Pools, (2018) Journal of European Consumer and Market Law 4, p. 146, 150). Therefore, it has been suggested that the shared data may have to be limited in scope, or aggregated and anonymized (Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, "Competition policy for the digital era," 2019, p. 96), which could be achieved by the establishment of a data escrow under this Principle that supplies data without any indications as to the companies it comes from.

d. Default terms and *f. Analogies.* In Europe, data escrow contracts are mostly classified as a "trust," which is defined as a "legal relationship in which a trustee is obliged to administer or dispose of one or more assets in accordance with the terms governing the relationship to benefit a beneficiary or advance public benefit purposes" (see Article X. – 1:201 DCFR). Therefore, reference can be made to the Reporters' Notes in Principle 13.

Principle 15. Data Marketplace Contracts

(1) A data marketplace contract is a contract between a party seeking to enter into a data transaction (the "client") and a data marketplace provider, under which the data marketplace provider undertakes to enable or facilitate "matchmaking" between the client and other potential parties to data transactions and, in some cases, provide further services facilitating the transaction.

(2) Subject to agreement of the parties and to other principles that take priority under Principle 5, the law should provide that the following terms are included in a data marketplace contract:

(a) insofar as the data marketplace provider undertakes to facilitate or enable a particular step with regard to a transaction, it must provide reasonable support to the client in complying with any legal duties applicable to that step;

(b) the data marketplace provider must refrain from any use for its own purposes of data, received from its client, that is the subject of the anticipated transaction; and

(c) upon full performance or termination of the contract, the data marketplace provider must erase any data in its control that is the subject of the anticipated transaction and that it has received from its client, and any data derived from such data.

(3) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to data marketplace contracts, consideration should be given in particular to:

(a) whether, and the degree to which, the data marketplace provider gains control of the data concerned; and

(b) whether, and the extent to which, the payment or other performance owed to the data marketplace provider depends on the whether the matchmaking results in a data transaction.

Comment:

a. Scope. Data marketplaces play an important role in the data economy. They can connect suppliers and recipients of data that, without the help of an intermediary, would not normally be able to find each other and enter into a data transaction without undue burden or expense. The most common transactions facilitated by such intermediaries are contracts for the transfer of data within the meaning of Principle 7, followed by contracts for access to data within the meaning of Principle 8. A "data marketplace provider" is defined, for the purposes of these Principles, as an intermediary who engages in "matchmaking" (i.e., acts as an intermediary facilitating transactions between suppliers and recipients of data). Usually, data marketplaces provide a range of further services to the parties, such as providing the infrastructure for transferring the data and any payment, assisting the parties in complying with legal requirements, and providing reputational ranking services or services related to complaint handling. There are many types and business models, such as "one-to-one," "one-to-many," and "many-to-many" marketplaces. This Principle can be applied to each of these models. Some marketplaces have control of the data supplied, while others restrict themselves to the matchmaking between supplier and recipient.

When data is supplied via a data marketplace, there are usually three contractual relationships involved: the relationship between the supplier and the recipient, the relationship between the supplier and the marketplace, and the relationship between the marketplace and the recipient. Both the relationships between the supplier and the marketplace and between the recipient and the marketplace are marketplace contracts within the meaning of this Principle.

Illustration:

82. Truck fleet operator T wants to minimize the amount of time lost to required rest breaks and meal breaks taken by its drivers. Through geolocation devices on T's trucks, T is aware of where its trucks are at all times but does not always know the most efficient routing for those trucks to make sure that they are near appropriate rest and food locations at the best time for breaks. T enters into a contract with intermediary I under which I agrees to find a party that can supply real-time data as to rest and food locations and estimated travel time to them in light of current weather and traffic conditions so that T can use this information to direct its trucks to the most efficient locations for rest and meal breaks. The contract between T and I is a data marketplace contract.

b. Default terms. As with other data contracts, this Principle provides several default terms for data marketplace contracts. Each of the four supplied default terms imposes a duty on the data marketplace provider. Paragraph (2)(a) obligates the provider to assist the client in complying with legal duties that apply to the transaction facilitated by the data marketplace provider.

Paragraph (2)(b) obligates the data marketplace provider to refrain from processing for its own purposes any data that is the subject of a data transaction that it enables or facilitates.

Paragraph (2)(c) obligates a data marketplace provider who enters into a data marketplace contract to erase any data in its control that is the subject of the anticipated transaction and that it has received from its client, and any data derived from such data, upon full performance or termination of the contract.

Illustration:

83. P runs a website on which users can search for hotels available in a particular location on a particular date and compare accommodations and prices. This service enables P to amass significant data concerning the number of people who are considering travel to those locations on particular dates. P believes that this information would be very valuable to car rental companies that have dynamic pricing models so they can adjust their rates in those locations based on anticipated demand. P does not, however, have the expertise necessary to identify the appropriate officials of car rental companies to propose entering into data transactions with them. Accordingly, P enters into a contract with data marketplace provider I pursuant to which I performs matchmaking between P and car rental companies to enable P to enter into data transactions with those companies. To enable I to

perform its matchmaking most effectively, P supplies some of its data to I. When the contract between P and I has been fully performed by I, or has otherwise been terminated, I must erase the data supplied to it by P.

c. Application of other law by analogy. Contracts with a party that provides matchmaking services are well known in a number of contexts outside the scope of these Principles. For example, parties wishing to sell real property often contract with matchmakers to find buyers for the real property, and potential buyers will often similarly contract with matchmakers to find appropriate real property within the buyer's budget. Similarly, companies seeking loans often contract with matchmakers that can match them with lenders that make loans to other companies in similar circumstances. To the extent that, in the applicable jurisdiction, default rules and principles have been developed for application to such matchmaking contracts, those rules and principles are appropriate to apply to data marketplace contracts by analogy. In some jurisdictions, those legal rules and principles differ depending on whether compensation is owed to the matchmaker only if the matchmaking services are successful and whether the matchmaker obtains control over the subject matter of the match.

Illustration:

84. R runs a website containing reviews and rankings of various consumer products. R harvests location data with respect to customers who access reviews and rankings. Data as to the number of such customers seeking information about consumer products in a particular location has value to retailers in that location. R enters into a data marketplace contract with intermediary I pursuant to which I will be paid a fee for each successful match between R and a retailer with respect to such data; the fee is an agreed fraction of the amount charged by R to the retailer. Under the data marketplace contract, I receives no compensation except for the fee for successful matches. In determining what legal rules and principles to apply by analogy to the data marketplace contract, reference should be made to rules and principles developed for other similar matchmaking contracts and, in particular, to those in which the matchmaker's compensation is determined by the number and magnitude of successful matches.

REPORTERS' NOTES

United States:

In the United States, a data marketplace contract is governed by the general law of contracts (see generally Restatement of Law Second, Contracts (AM. L. INST. 1981)). As is the case with all contracts, courts may supply contractual terms to address matters not addressed by the parties. See id. § 5, Comment *b* ("Much contract law consists of rules which may be varied by agreement of the parties. Such rules are sometimes stated in terms of presumed intention, and they may be thought of as implied terms of an agreement."). Restatement of the Law Second, Contracts § 204 further provides that "When the parties to a bargain sufficiently defined to be a contract have not agreed with respect to a term which is essential to a determination of their rights and duties, a term which is reasonable in the circumstances is supplied by the court." Id. § 204. Thus, paragraph (2) of this Principle can be seen as an enumeration of reasonable terms to be applied to the issues addressed in the absence of agreement of the parties.

An increasing number of data marketplaces are available online. See, e.g., the IOTA Data Marketplace, which can be viewed at https://data.iota.org/#/. For a discussion of enhanced matchmaking services, see, e.g., Marshall W. Van Alstyne & Michael Schrage, *The Best Platforms Are More than Matchmakers*, HARV. BUS. REV. ONLINE (2016), https://hbr.org/2016/08/the-best-platforms-are-more-than-matchmakers.

Europe:

a. Scope. The regulation of online platforms is one of the milestones the European Commission has announced in its Digital Single Market Strategy (COM(2015) 192 final, p. 11 ff). A first major step was the adoption of the Platform to Business Regulation (P2B) (Regulation (EU) 2019/1150), which mainly contains transparency obligations. The Data Governance Act (DGA) (Regulation (EU) 2022/868) establishes notification requirements and conditions for data intermediation service providers. Data intermediation services covered by the DGA include intermediation services between data holders that are legal persons and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users (Article 10(a)). This would fall under the notion of a data marketplace within the meaning of this Principle. Data marketplaces normally also qualify as an "online platform" within the meaning of the Digital Services Act (DSA) (Regulation (EU) 2022/2065), see Article 3(i) of the DSA. The DSA mainly contains exemptions of liability and due diligence obligations for all providers of intermediary services and the due diligence obligations are—at least under the proposal—only to be enforced by public authorities.

The fact that online platforms may as well provide additional services with regard to data is also recognized by the DGA, which explicitly allows providers of data intermediation services to offer additional services to facilitate the exchange of the data, such as storage, curation, pseudonymization, and anonymization (see Article 12(e) DGA).

b. Default terms. The obligation under paragraph (2)(a) of this Principle—that the data marketplace provider that facilitates certain steps of the transaction must provide reasonable support to the client in complying with any legal duties—would, under most European jurisdictions, be classified as an ancillary obligation to the contract. Specifically with regard to data, similar obligations can be found in the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), e.g., among the obligations owed by a processor vis-à-vis the controller. According to Article 28(3) of the GDPR, the processor must, inter alia, assist the controller by taking appropriate technical and organizational measures, insofar as that is possible, to respond to requests by data subjects to exercise their rights and to enable compliance with legal obligations, taking into account the nature of processing and the information available to the processor. This is also the idea underlying Article 31 of the DSA. Due to the fact that many obligations in e-commerce can only be fulfilled with the help of the intermediary, the proposal sets out that the providers of online platforms "shall ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information under applicable Union law."

Paragraph (2)(b) of this Principle—which obligates marketplace providers to refrain from any processing of the data that is the subject of the marketplace contract for their own purposes—has similarities to the default rule set out in Principles 12(2), 13(3), and 14(3) and in the Data Governance Act. The latter sets out a duty for providers of data intermediation services to act in the data subjects' best interests when facilitating the exercise of their rights, and to not use the data for other purposes than to put them at the disposal of the data users (Article 12(m) DGA).

Restrictions on the continued use of data after termination of the contract (paragraph (2)(c) of this Principle) can also be found in Principle 12(2)(e). In European law, Article 28(2)(g) of the GDPR provides that the processor must delete or return all personal data to the controller after the end of the provision of services relating to processing. Furthermore, the controller has the duty to erase personal data without undue delay when the personal data are no longer necessary in relation to the purposes for which they were collected (Article 17(1)(a)). When a trader supplies digital content or services to a consumer, Article 16(3) of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) stipulates that upon termination of the contract, the trader shall refrain from further use of the content, which is data provided or created by the consumer when using the digital content or service supplied by the trader.

c. Application of other law by analogy. In Europe, data marketplace contracts under this Principle would generally be classified as service contracts (see the Reporters' Notes to Principle 12).

PART III
DATA RIGHTS

CHAPTER A
RULES AND PRINCIPLES GOVERNING DATA RIGHTS

Principle 16. Data Rights

(1) Data rights may include the right to:

(a) be provided access to data by means that may, in appropriate circumstances, include porting the data;

(b) require the controller to desist from data activities;

(c) require the controller to correct data; or

(d) receive an economic share in profits derived from the use of data.

(2) The data rights set out in Part III are not exhaustive; rather, a legal system may conclude that parties should have additional rights of this sort. Accordingly, no negative inference should be drawn from the absence of those rights in Part III.

(3) The rights set out in Part III are without prejudice to rights other than data rights that a person may have against a controller of data with regard to that data, such as rights arising from breach of contract, unjust enrichment, conversion of property rights, or tort law.

Comment:

a. The concept of data rights. The Principles in Part III deal with legally protected interests that arise from the very nature of data as information recorded in a machine-readable format suitable for automated processing, stored in any medium or as it is being transmitted (Principle 3(1)(a)); they do not, however, address intellectual property rights that may exist in certain data (Principle 1(2)). Data as recorded information is a non-rivalrous resource, which may be used by many different parties for many different purposes at the same time, and to the generation of which many parties may have contributed in many different ways. These attributes are taken into account as the foundation of a set of Principles that recommend the recognition of a new data-specific class of rights, which may be called "data rights." Rights of this nature are being recognized to an increasing extent in data-specific legislation and case law worldwide, mostly taking the form of access rights. These data rights are not purely contractual, as they may exist between parties

without any contractual link and they do not reflect ownership notions in the traditional sense because traditional notions of ownership do not work well with resources of a non-rivalrous nature.

Illustration:

85. Small airline A operates airplanes manufactured and sold by P, the engines for which were supplied by engine manufacturer E. Data concerning the performance of the engines is transmitted directly from the connected engines to D, a data analytics company developing predictive maintenance services and belonging to the same group of companies as E. A would like to have access to the engine data in order to get a better idea of whether maintenance could be dealt with in a more cost-efficient way. Part III deals, inter alia, with questions such as whether A has a data right as against D to be given access to certain data concerning performance of the engines in airplanes run by A. This right would not arise from contract as there is no contract between A and D, and not even between A and E. Without a data right to access to the data of the sort recommended by these Principles, in order to obtain access to the engine data A would need to insist on a term, in its contract with P to obtain the airplanes, that would require P to include in its contract with E a right of buyers such as A to access the data supplied to D. Requiring A to negotiate for this cascade of contracts, sometimes referred to as "going along the links of the chain" would be unduly costly and time-consuming. Besides, existing contracts that P has with E, and that E has with D, may not be readily renegotiated.

b. Typical data rights. The most important type of data right, and the type that is the most specific to the nature of data as a non-rivalrous resource, is the right to access data. Given the broad definition of "access"—which may mean anything from merely being able to read data to being able to engage in varying degrees of processing the data on a medium in the controller's sphere to full portability of the data—access rights may come in many different forms. It is, however, not feasible for these Principles to differentiate between those many different shades of "access." Rather, these Principles deal with access rights in general, allowing for flexibility as concerns the modalities of access.

Another important data right may be the right to require that a party desist from particular data activities, which can include a right to require desistance from any control or processing of data, i.e., to require erasure of data. This, too, is a right that is specific to the nature of data, in this case, the nature of data as a resource the generation of which many different parties have

contributed to in many different roles, and the use of which is in a way not usually seen in the tangible world or with other more traditional assets.

A related data right is the right to require correction of incorrect or incomplete data. Finally, these Principles consider an exceptional right to require an economic share in profits derived from the use of data. This, again, is specific to the nature of data as a resource the generation of which parties have contributed to even if they did not volunteer to contribute or were unaware that they were contributing, and therefore did not have a fair chance to negotiate for remuneration.

There may be other, related data rights not specifically listed in paragraph (1) of this Principle, such as the right to receive information about data held by a particular controller, which may be of a procedural nature in some jurisdictions and a matter of substantive law in others.

c. Difference between data rights under Chapters B and C. Most of these rights, as set out in Chapter B on rights in co-generated data, are justified by the share that a party had in the generation of the data that is at stake: A party can have a share in the generation of data by providing part of the content of the information coded in the data—e.g., the information is about something that party has done or is likely to do—or by generating the code—e.g., that party drives a connected car and that activity causes large amounts of information to be recorded—or by otherwise providing a contribution to data generation within the meaning of Principle 18(1). Given that the share a party had in the generation of data may justify very different data rights as listed in paragraph (1) of this Principle, the range of rights addressed in Chapter B is broad and diverse.

The data rights dealt with under Chapter B fulfill functions similar to those fulfilled by ownership with regard to traditional rivalrous assets. However, the question of whether the bundle of rights in co-generated data constitutes "property" or "ownership" is not addressed by these Principles, as these Principles focus on the nature of the rights and not on their doctrinal classification. Rights in co-generated data reflect a policy that whoever has contributed to the generation of data should generally have some rights with respect to its use or with respect to the value it generates. Unlike intellectual property rights, rights in co-generated data do not afford their holder a clearly defined range of rights against everyone else to do something or to omit doing something, but rather the data rights depend very much on the parties involved, and on the particular situation.

As contrasted with the data rights addressed under Chapter B, which fulfill functions similar to those fulfilled by ownership, those addressed in Chapter C are of a very different nature. They are typically afforded to persons who did not have a share in the generation of the data but who

should nevertheless have a data right for other overriding considerations of a more public law nature. Data rights within the meaning of Chapter C are, in reality, almost exclusively data access rights, but might theoretically also include other forms of data rights.

While there is a clear theoretical distinction between the justification for data rights in co-generated data and the justification for data rights for the public interest, the distinction is not always as clear in the context of specific situations. For example, a data right that primarily serves a public interest (e.g., fostering competition and innovation) may be afforded to a party that contributed to the generation of the data. This is a constellation we often find in the context of statutory portability rights, in which the legislator may primarily have the benefit for third-party recipients of data in mind, but nevertheless chooses (portability) rights in co-generated data as a tool to achieve this aim. If this is the case, legislators or courts may want to take into account the Principles of both Chapter B and Chapter C.

d. Nonexclusive character. Part III sets out in some detail matters with respect to which the law should provide for data rights. However, Part III is not intended as an exclusive list of such rights. Rather, some states might decide that additional data rights should be recognized now, and as the data economy develops and matures, states may well recognize further data rights and related rights. Such related rights may facilitate the assertion of a data right in the first place, e.g., by giving a right to be informed of whether the controller holds relevant data. paragraph (2) of this Principle clarifies that these Principles do not exclude the existence of such additional data rights and related rights.

In a very similar vein, paragraph (3) of this Principle clarifies that Part III is without prejudice to any other rights (i.e., rights that cannot genuinely be classified as "data rights") following from existing bodies of the law, such as arising from breach of contract, unjust enrichment, conversion of property rights, or tort law, insofar as these rights might also arise in a data context.

REPORTERS' NOTES

United States:

As a general matter, it is almost axiomatic that U.S. law does not regulate the fairness of arms'-length relationships as such. See, e.g., P.S. Atiyah, *Contract and Fair Exchange*, 35 U. TORONTO L.J. 1 (1985) (part of the traditional dogma of contract law is that "[t]here is simply no room for any inquiry into the fairness of the exchange"). There are quite a few exceptions to that generalization, however. To mention just a few, transactions between corporations and their

directors are often subjected to a fairness test (see, e.g., Lawrence E. Mitchell, *Fairness and Trust in Corporate Law*, 43 DUKE L.J. 425 (1993)), as are other matters between a fiduciary and a beneficiary.

In the context of transactions, the primary consideration of this sort comes from the doctrine of unconscionability, which empowers judges to decline to enforce certain oppressive arrangements. See Uniform Commercial Code (UCC) §§ 2-302 and 2A-108 (2021-2022 ed.); Restatement of the Law Second, Contracts § 208 (AM. L. INST. 1981). While the nature of what constitutes unconscionability is the subject of much controversy (see, e.g., Restatement of the Law, Consumer Contracts § 5 (AM. L. INST. forthcoming)), it is generally agreed that demonstrating unconscionability requires more than showing that the arrangement is one-sided as a result of an imbalance in bargaining power. See, e.g., UCC § 2-302 ("The principle is one of the prevention of oppression and unfair surprise and not of disturbance of allocation of risks because of superior bargaining power.") (internal citations omitted).

Also, while there is general recognition that contracts of adhesion raise issues that do not arise in fully bargained contracts between those with comparable bargaining power, U.S. jurisdictions differ as to the appropriate judicial response to that phenomenon.

Finally, the recognition that each party to a contract has a duty of good faith and commercial reasonableness (see UCC § 1-304; Restatement of the Law Second, Contracts § 205 (AM. L. INST. 1981)) constrains much behavior that might otherwise seem to be allowable under a narrow reading of transactional documents. See PEB Commentary No. 10 (1994) (explicating UCC concept of good-faith performance). See also Robert S. Summers, *Good Faith in General Contract Law and the Sales Provisions of the Uniform Commercial Code*, 54 VA. L. REV. 195 (1968).

Europe:

Around the world, the notion of "data rights" is becoming a central element in academic discussions on creating a robust legal framework for the data economy (see, e.g., Yuming Lian, Data Rights Law 1.0, 2019, pp. 105 ff, 155 ff). The existing legal framework on data rights is fragmented and consists of a range of different instruments addressing specific issues in the data economy. Thus, existing data rights in the European Union have, so far, largely not been guided by an overarching consideration or aim to address data economy issues on a horizontal basis. With the recent proposal for a Data Act (DA) (COM(2022) 68 final), the European Commission intends to provide for a coherent and horizontal approach to data rights. Besides provisions on business-to-government (B2G) data sharing, the Data Act contains—as was already envisaged by the European Commission in the Data Strategy (COM(2020) 66 final, pp. 13, 26 et seq.)—a data access and a data portability right for users with regard to the data generated by their "Internet of Things" (IoT) devices (Articles 3 ff DA), horizontal obligations for data holders legally obliged to make data available (Articles 8 ff), and an unfairness test for business-to-business (B2B) data access and use contracts (Article 13 DA). That approach by the European Commission is clearly aligned with the concept of data rights in relation to co-generated data set out in Part III, Chapter B, of these Principles. However, unlike these Principles, the Data Act's provisions on data access and use presuppose that the controller and the party seeking a data right are in a contractual relationship. Moreover, the Data Act is much narrower in scope than Part III of these Principles, as the latter

address any data that has been co-generated by multiple actors while the Data Act proposal only applies to data that has been co-generated in IoT-settings.

Portability and access rights are closely related, but the exact delineation between the two concepts is subject to scholarly debate (see Yannic Duller, Facilitating Access to Data Silos (forthcoming); Sebastian Schwamberger, Der Datenzugang (forthcoming)). In the proposal for a Data Act, the European Commission distinguishes between "the right of users to access data generated by use of products and related services" under Article 4 and the "right to share data with third parties" under Article 5. Both rights should be fulfilled without undue delay, free of charge to the user and, when applicable, continuously and in real time. The main difference between those two rights is that under the former, the data needs to be made available to the user, whereas under the latter, the data needs to be made available to a third party upon request by a user, or by a party acting on behalf of a user. Consequently, whether it is a right to access or a right to share depends on who is granted access to the data. If data access is granted to the "user," it is a data access right, but if the access is granted to a third party at the request of the user, it is a data sharing (portability) right.

Besides Articles 4 and 5 of the proposal for a Data Act, it is undisputed that the most prominent "portability rights" are Article 16(4) of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) for non-personal data and Article 20 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) for personal data. Pursuant to Article 20 of the GDPR, data subjects have the right to receive personal data concerning them, which they have provided to a controller on the basis of consent or a contract, in a structured, commonly used, and machine-readable format, and to freely transmit that data to another controller. If technically feasible, data subjects may request that the personal data be transferred directly from one controller to another. The right to access data can also be found in several sector-specific regulations. (See, e.g., Article 61 Payment Services Directive II (Directive (EU) 2015/2366); Article 12 Electricity Directive (Directive (EU) 2019/944); Article 66 ff Type Approval Regulation (Regulation (EU) 2018/858); Article 27 of the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation (Regulation (EC) No 1907/2006).) While the former two access rights aim to avoid anti-competitive lock-in effects to the detriment of customers, and would thus be classified as Chapter B rights (see Rapporteur's comments on Principle 20), the latter two rights would fall under Chapter C as they are justified by public interest rather than co-determination considerations (see Rapporteur's comments on Principle 24). Finally, the Digital Markets Act (DMA) (Regulation (EU) 2022/1925) contains data access and portability obligations, based on considerations of co-generation, in Article 6(9) and (10).

The right to require a controller to refrain from controlling or processing data appeared for the first time in data protection law (see Article 12(b) and Article 14 of the predecessor Directive 95/46/EC of the GDPR). Pursuant to Article 17 of the GDPR, data subjects may request a controller to erase data relating to them. In particular, the data subject has that right if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed, or if consent to the processing has been withdrawn and there is no other legal basis for the processing. Under the GDPR, data subjects may also request restriction of processing instead of erasure (see Article 18). However, with the advent of the data economy, the right to obtain an injunction has

gained importance beyond data protection law and has also been incorporated into European contract law. Due to the non-rivalry of data, the right to demand the cease and desist of data processing fulfills a similar function as the right to reclaim physical goods. In the event of termination of the contract for the provision of a digital service/content, Article 16(3) of the DCSD requires the trader to refrain from using content other than personal data provided or created by the consumer when using the digital content or digital service provided by the trader.

The most prominent example for a "right to receive information," as mentioned in the Comments, is Article 15 of the GDPR. That provision entitles data subjects to receive information on whether or not personal data concerning them are being processed, and, when that is the case, access to the personal data in form of a copy (Article 15(3)). In addition, the data subjects are to be informed about the existence of their rights to rectification, or erasure of the data under Article 17 of the GDPR. Thus, Article 15 of the GDPR enables certain data rights to be enforced in the first place, but does not grant access to the data within the meaning of these Principles.

Principle 17. Application of these Principles to Data Rights

Rights under Part III should be governed, in the following order of priority, by:

(a) rules of law that cannot be derogated from by agreement, including data privacy/data protection law;

(b) agreement between the parties to the extent that the contract is consistent with Principles 18 to 27 or there is freedom of the parties to derogate from Principles 18 to 27 under the applicable law;

(c) any applicable rules of law other than those referred to in subparagraph (a) that have been developed for application to data rights; and

(d) Principles 18 to 27.

Comment:

a. Hierarchy of sources. This Principle fulfills, for data rights, a function similar to that fulfilled by Principle 5 for data contracts; it sets out a general framework for the law governing data rights and identifies the order of priority of the various possible sources of rules governing those rights.

As with Principle 5 for data contracts, mandatory rules of the applicable law take absolute priority over rules from any other sources. Such mandatory rules may be rooted in concepts of inalienable rights. They may, in particular, have their origin in data protection/data privacy law, or, at least to a certain extent, in trade secrets law. Several regimes of protection of personal data (data privacy) worldwide have introduced quite far-reaching access rights, porting rights, and rights

to request erasure or rectification of data, plus some other rights, such as restriction of processing. These rights are vested in the data subject, i.e., the person to whom the personal data is referring. Their logic is, notably in Europe, predominantly a fundamental human rights logic, but partly also a property or competition law logic. Such rights, which cannot be derogated from by agreement, are not affected by Principles 18 to 27, but Principles 18 to 27 may still be useful for their interpretation and for gap-filling.

Illustration:

86. P frequently uses the services of platform operator O. When establishing an account on the platform, P accepted O's data protection terms, including a term stating "I agree that O may use my personal data for personalizing the content I see and the offers I receive, and that for said purpose O will also pass my data on to third parties." Later, when P engages in online shopping, P receives offers exactly calculated to match P's estimated maximum ability and willingness to pay, using, inter alia, data from P's personal diary (which indicates, e.g., when P has commitment to be at distant locations and needs an airplane ticket or the like to get there) with the result that P, on average, pays 30 percent more than P would have paid if offers had not been personalized. At first sight, P may be seen as having given consent, but Principle 21 may provide arguments that consent should not be seen as valid (under doctrines of applicable law, such as doctrines of unconscionability or unfairness), or that consent should be interpreted as not covering the data utilization at hand.

Next, this Principle lists the agreement of the parties as a source of relevant rules and principles. The conditions under which a person has a data right, and in particular the details of such right, should ideally be defined in an agreement between the parties involved. However, an agreement should govern only to the extent that it is consistent with Principles 18 to 27, considering any need for interpretation or gap-filling, or to the extent that applicable law allows parties the freedom to derogate from Principles 18 to 27 by agreement.

Illustration:

87. Assume that, in the situation described in Illustration no. 85, a contract between airline A and engine manufacturer E explicitly excludes any kind of rights on the part of A to access engine data. This contract would presumably—depending on the circumstances

of the individual case—be inconsistent with Principle 20. Whether or not it supplants the rights provided in Principle 20 would depend on the extent to which Principle 20 is subject to waiver. According to Principle 16(2) this depends on the (otherwise) applicable law, i.e., it is only to the extent that the applicable law allows for such data rights to be waived by way of contract that the contract would override Principle 20. In any case, Principle 20 might be an argument for interpreting any contract clause on waiver rather narrowly.

Next in order of priority come any rules of law other than those referred to in subparagraph (a), i.e., other than mandatory, that have been (specifically) developed for data rights. As yet, there seems to be no general ("horizontal") statutory regime of data rights, nor a regime created by case law. However, this is in flux, and there are an increasing number of access rights and similar rights in particular sectors, such as in the financial, energy, and mobility sectors, and/or developed on the basis of competition law.

When there are no mandatory laws, contractual provisions that override these Principles, or specifically designed legal rules other than mandatory laws, this Principle recommends that rights should be governed by Principles 18 to 27. According to Principle 16(2) this could occur within existing legal frameworks.

REPORTERS' NOTES

United States:

See generally the Reporters' Notes to Principle 5, explaining the hierarchy of legal principles applicable to contracts.

With respect to rules that cannot be derogated from by agreement, see Principles of the Law, Data Privacy § 4 (AM. L. INST. 2020). As stated in the Reporters' Notes to that Section, "American information privacy law generally makes its notice requirements mandatory, and not subject to waiver by the affected individual." Id., Reporters' Note *1*. See also CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798.192: "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

For examples of remedies with respect to data rights, see, e.g., Principles of the Law, Data Privacy § 14 (AM. L. INST. 2020) and the extensive analysis of source material in the Reporters' Notes to that Section. See also, e.g., CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798.150.

Europe:

In Europe, the majority of specific statutory regimes on data rights are of a mandatory nature. This applies to the rights in Article 16(4) of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770); Articles 61 ff of the Type Approval Regulation (Regulation (EU) 2018/858), Article 12 of the Electricity Directive (Directive (EU) 2019/944); Articles 66 f of the Payment Sector Directive II (PSD II) (Directive (EU) 2015/2366); and Articles 15 ff of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

However, statutory regimes of data rights also interact with contractual agreements. An interesting illustration for this interplay is Title III (Articles 25 to 30) and Articles 118 and 119 of the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation (Regulation (EC) No 1907/2006). In order to strengthen the competitiveness of the European industry, to avoid unnecessary testing (including on animals), and to ensure that the Regulation is applied as efficiently as possible, provision is made for the sharing of data between registrants on the basis of fair compensation. If a substance has previously been registered less than 12 years earlier, the potential registrant shall, in the case of information involving tests on vertebrate animals, and may in other cases, request from the previous registrants certain information he or she requires. The potential and previous registrant(s) shall make every effort to reach an agreement on the sharing of the information requested. Such an agreement may be replaced by submission of the matter to an arbitration board and acceptance of the arbitration order. The previous and potential registrant(s) shall make every effort to ensure that the costs of sharing the information are determined in a fair, transparent, and non-discriminatory way. In order to allow a potential registrant to proceed with the registration, even if an agreement with a previous registrant cannot be reached, the European Chemicals Agency, on request, should allow use of any summary or robust study summary of tests already submitted.

CHAPTER B
DATA RIGHTS WITH REGARD TO CO-GENERATED DATA

Principle 18. Co-Generated Data

(1) Factors to be taken into account in determining whether, and to what extent, data is to be treated as co-generated by a party within the meaning of Principles 19 to 23 are, in the following order of priority:

(a) the extent to which that party is the subject of the information coded in the data, or is the owner or operator of an asset that is the subject of that information;

(b) the extent to which the data was produced by an activity of that party, or by use of a product or service owned or operated by that party;

(c) the extent to which the data was collected or assembled by that party in a way that creates something of a new quality; and

(d) the extent to which the data was generated by use of a computer program or other relevant element of a product or service, which that party has produced or developed.

(2) Factors to be considered when assessing the extent of a contribution include the type of the contribution, the magnitude of the contribution (including by way of investment), the proximity or remoteness of the contribution, the degree of specificity of the contribution, and the contributions of other parties.

(3) Contributions of a party that are insignificant in the circumstances do not lead to data being considered as co-generated by that party.

Comment:

a. The concept of data rights in co-generated data. Principles 18 to 23 reflect the most important type of data rights: data rights based on the notion of co-generation of data. A common denominator of these rights is that they find their justification in the share that a party had in the generation of the data that is at stake: A party can have a share in the generation of data by being the subject of the information coded in the data, or by being the owner or operator of something that is the subject of the information, or by otherwise providing a contribution to data generation within the meaning of paragraph (1). The reference to "operator" in this Principle is to be understood as referring to lessees or similar persons operating the relevant object in their own names and on their own accounts. The share that the party had in the generation of the data is,

however, rarely the only justification. Rather, it is the share, together with the other factors listed in Principle 19(2) and further elaborated in Principles 20 to 23, that causes the data right in question to arise. However, when a party does not have any kind of share in the generation of data, not even by having invested in a data-generating device (which is the lowest-priority factor in the list provided by paragraph (1)), a data right asserted by that party would not be based on Principles 18 to 23.

Whether only individual parties who have themselves contributed to the generation of data (or their successors in interest, e.g., in a case of inheritance, merger, or acquisition) can rely on Principles 18 to 23, or whether also groups of persons, such as the citizens of a particular state, are protected by these Principles is a difficult question, as is whether there are circumstances under which one party can rely on a contribution made by another party.

Illustration:

88. Huge amounts of data generated by the citizens of a particular state is used by businesses from another continent to develop sophisticated digital services and digital products, which are then again sold to the citizens of the state of origin at a high price. Businesses from the state of origin of the data do not have the practical ability to develop services of their own because they do not have access to the necessary data. In scenarios such as this, the question arises whether this state, or businesses resident in this state, can assert the rights stated in Principle 20, arguing that "their" population has generated the data.

While these Principles do not rule out that such collective data rights may exist, see Principle 16(2), they do not address these rights.

b. General factors. Paragraph (1) is about the factors that determine what counts as co-generation of data. The notion of "co-generation" of data is a normative notion that does not coincide with any notions of "generation" of data that may be used in a more technical context. This becomes visible in the first factor listed in paragraph (1) for determining whether data is co-generated by a party—whether the party is the subject of the information coded in the data (e.g., personal data, or data relating to a particular business and its activities), or is the owner or operator of the subject of that information (e.g., data relating to the maintenance status of a machine, or to the quality of a piece of land). While, from a technical point of view, such a person would not be considered as having any share in the "generation" of data unless that person has at the same time

contributed to recording the binary code or the like, the law may take a broader perspective. Being the subject of the information may, from a legal point of view, even be the strongest form of contribution, depending on the specific link between the information and the legitimate interest in being provided access, etc., or requiring desistance, correction, or an economic share.

Another form of contribution of a party to the generation of data is that party pursuing an activity by means of which data has been produced (e.g., that party has driven a connected car) or owning or operating the device by means of which data has been produced (e.g., the party owns the machine that has generated the data). However, there are also other ways in which a party can produce data by its activity, including by processing existing data in a way that potentially adds value and makes it "new" data. This is why this Principle must not be (mis)understood as applying exclusively to the "first" producer of data, but rather as applying to any producer.

Largely the same considerations apply to any party that does not produce data in the strict sense of recording information that had not been recorded before but that assembles or structures existing data in a way that creates something of a new quality, e.g., a database.

A party may have contributed to the generation of data in other ways as well, such as by having produced or developed a computer program or other relevant component of a product or service.

Illustration:

89. User U is the owner of a connected car manufactured by P. Through the use of the connected car by U, a large amount of data is generated, some of it related to the status of the car itself (e.g., for purpose of predictive maintenance), some related to U's driving habits (e.g., for targeted advertising or dynamic insurance models), and some related to the environment (e.g., weather and traffic data). Since the data has been generated by an activity of U and the car that generated the data is also owned by U, U has a share in the generation of this data. P also has a share in the generation, as P developed and produced the car that generates the data and structures the data in a meaningful way. Thus, all of this data qualifies as having been generated by both U and P (and possibly by other parties).

Paragraph (1) lists these factors and also states that the share that a party had in the generation of data is to be assessed with a view to the degree of presence of these factors. Paragraph (2) clarifies that the share a party had in the generation of data depends on the type of contribution (i.e., which and how many of the factors listed in paragraph (1) of this Principle are fulfilled), the

remoteness of the contribution (e.g., when an individual provides personal data to a controller the share in the provided data is extremely high, but once the data has been pseudonymized or even anonymized, the share becomes smaller and smaller), and the specificity of the contribution (e.g., when the same contribution could have been made by any other party, it has less weight than when a contribution is specific for a particular party). Of course, the share also depends on the contributions of other parties (e.g., the controller that has processed data in order to obtain derived data, or that has inferred data from other data, may have a significant share in the generation of that data, the extent of that share depending on similar factors as the ones just mentioned).

The factors partly reflect considerations of personality rights, partly reflect the "labor theory of property," and partly follow from the idea that the proceeds of property should normally belong to the owner of the original property. The factors are listed in the order of their relative weight. This does not mean an absolute order of priority, but a factor that figures lower in the list normally needs to be present to a higher degree in order to have the same force as a factor that figures higher. Very often, more than one factor is present in a particular case, e.g., when a party generates data by driving their connected car, such data is at the same time identifiable to that party and to a device owned by that party, in which case that party has co-generated the data both under paragraph (1)(a) and paragraph (1)(b) and the contribution is potentially a particularly strong one.

Illustration:

90. In Illustration no. 89, the share that U had in the generation of all three types of data mentioned (status of the car, driving habits, environment) is quite high as it was by U's activity of driving the car, and by the data collecting functions of the car as a device owned by U, that the data has been recorded. However, U's share in generating the data on personal driving habits is greatest, given the high degree of proximity and specificity and the absence of comparably significant contributions from other parties. As compared with U's share in the other data types, the share in the generation of the weather and traffic data is smallest. This is so because the data does not specifically relate to U or to U's car, and because manufacturer P's contribution by designing the car's sensors in a way that this data is collected is significant in this case.

c. Insignificant contributions. Paragraph (3) clarifies that contributions of a party that are insignificant in the circumstances do not lead to data being considered as co-generated by that

party. This is to avoid uncertainty and a situation in which a controller of data is confronted with an incalculable number of parties asserting data rights based on a remote or minor contribution.

Illustration:

91. In Illustration no. 89, traffic data is also, to some extent, generated by other traffic participants, and all data types mentioned are generated, to some extent, by all manufacturers who had anything to do with the development of relevant car components, such as the development of the car's sensors, etc. However, in the specific situation (and except when the dispute at hand is about, e.g., the manufacturer of the sensors seeking access to the data collected by the sensor), these contributions are so remote that they should be discounted.

REPORTERS' NOTES

United States:

While the term "co-generated data" is not typically used in the United States, there has been increased discussion of the legal issues raised by the concept that the term abbreviates. Very useful examinations and discussions of many of these issues can be found in Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220 (2018) (proposing a property rules construct that clearly defines rights to digital information that arise upon creation) and in Rob Frieden, *An Introduction to Data Property Ownership Rights and Data Protection Responsibilities* (Aug. 5, 2019), available at SSRN: https://ssrn.com/abstract=3432422 or http://dx.doi.org/10.2139/ssrn.3432422. While both papers advocate a regime based on property concepts to recognize rights in what these Principles refer to as "co-generated data," their description and analysis of the topic is valuable whether or not a legal regime chooses to establish a property rights regime to regulate it. Frieden notes that "Data often gets generated without the conscious effort of a person to create it. However, the absence of such data creation would foreclose the execution of a desired transaction or encounter." Id. at 5. As an example, he observes that:

> [W]ireless telephone and broadband network operators cannot complete a telephone call, or provide broadband-mediated access to an Internet web site without collecting data about the call or session originator's location, the identity of the intended call recipient, the originator's credit worthiness and subscription account information, etc. Elements of property ownership can apply to the above type of transaction, because the data generated, collected, stored, processed and analyzed also can accrue value in ways that have nothing to do with the completion of a telephone call, or initiation of an Internet data session. The data generated can provide details about people making telephone calls and accessing the Internet while also accruing new value even as it may intrude upon the person's reasonable

> expectation of privacy. Speedy and comprehensive analysis of other collected data can provide analysts with ways to identify many true, but private aspects about a person.

Id.

Ritter and Mayer, who, like Frieden, conclude that the regime that allocates rights with respect to co-generated data should be described as a "property rights regime," note that:

> [T]he following questions appear to apply both for industrial data and personal information: How should ownership of data be defined, if at all? When does ownership attach to data? Are there pre-conditions or criteria (such as originality, level of effort, or imposition of security controls) to be satisfied before ownership will be deemed to be attached to specific data? What are the rights, privileges, controls, and constraints that data ownership vests in the owner? How may those rights, privileges, and controls be transferred or regulated by contracting tools (such as purchase agreements and licenses)? What tools, mechanisms, or processes exist (or can be imagined) that may automatically enforce the rights, privileges, and controls of data ownership across distributed, complex information systems? Do existing, conflicting legal treatments of industrial data under copyright and database laws continue to work if clear ownership itself is defined now as an explicit starting point? How do certainty of ownership and the legitimate exercise of controls on the rights of ownership affect how data is economically valued as an asset of any company, business, or operating entity?

Ritter & Mayer, *Regulating Data*, at 227.

Frieden also notes that co-generation issues are particularly acute with respect to consumers.

> Consumers are the primary subjects for the creation of data even though they may not actively participate. Consumers create useable data by filling in forms and disclosing personal information, but much more data gets created by their public, private and commercial activities. This means that consumers may not know whether and how data is being collected about a specific activity. Without voluntary or mandatory disclosure by the data collector, consumers may not even know the nature and scope of what information has been acquired, processed, analyzed and marketed. Accordingly, consumers have an interest in who collects, data, what they collect, when they do so, how they use the data and with whom they can sell or otherwise exchange the data.

Frieden, *An Introduction to Data Property Ownership Rights*, at 24.

Europe:

a. The concept of data rights in co-generated data. The idea of shared value creation of data has been recognized by the European Commission in its Communication "Towards a common European data space" (COM(2018) 232 final, p. 10). This concept of non-exclusive rights in data competes with the idea, discussed for some time under the heading of "data ownership," to introduce an exclusive data right (for details see the Reporters' Notes to Principle 29). Meanwhile,

the idea to introduce such an exclusive right has largely been dropped, and the concept of co-generated data has gained widespread recognition. The concept of "co-generated data" developed by these Principles has already been adopted by the European Commission in its European Data Strategy (COM(2020) 66 final, p. 10), the German Data Ethics Commission (Opinion of the German Data Ethics Commission, 2019, p. 133 ff.), and the Global Partnership on Artificial Intelligence (GPAI) (see GPAI Working Group on Data Governance, A Framework Paper for GPAI's work on Data Governance, 2020).

The proposal for a Data Act (COM(2022) 68 final) puts forward several provisions that are based on the concept of co-generated data and the underlying notion that a party who had a share in the generation of the data should be afforded certain rights in regard to that data. According to Articles 4 and 5, users of "Internet of Things" (IoT) products or related services shall have the right to access and use data generated by the use of an IoT product or related service and to share the data with third parties. The data that is the subject of the access and sharing rights under the Data Act proposal is co-generated data within the meaning of this Principle, because it is generated by a device that is owned by the user and/or by an activity of the user (paragraph (1)(b) of this Principle). Furthermore, the data generated by the use of an IoT product will usually be information on the user (e.g., personal data, or data relating to a particular business and its activities), or an asset owned or operated by the user (paragraph (1)(a) of this Principle). Usually, not only the user will have made a contribution to the generation of the data but also the data holder. The data holder may have developed and produced the IoT product or related service (paragraph (1)(d) of this Principle) and/or structured the data in a meaningful way (paragraph (1)(c) of this Principle). The Data Act proposal also recognizes the legitimate interests of the data holder as well as third parties, e.g., by setting out that the user or third-party recipient may not use the accessed data to develop a product that competes with the product from which the data originates (Articles 4(4) and 6(2)(e) Data Act proposal; see further the Reporters' Notes to Principle 20).

The notion of co-generated data is also reflected in the unfairness control of contractual terms unilaterally imposed on a micro-, small-, or medium-sized enterprise (MSME) set out in Article 13 of the Data Act proposal. According to Article 13(4)(c), contractual terms that prevent an MSME from using the data contributed or generated by the MSME during the period of the contract, or limit the use of such data to the extent that the MSME is not entitled to use, capture, access, or control such data or exploit the value of such data in a proportionate manner are presumed unfair. A contractual term that prevents an MSME from obtaining a copy of the data, which was either generated by the MSME or to which it contributed, during the period of the contract or within a reasonable period after the termination thereof is also presumed unfair (Article 13(4)(d)).

b. General factors and *c. Insignificant contributions.* That a party's contribution to the generation of data is a very relevant factor for assigning data rights is particularly evident as far as personal data is concerned. Under the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), data subjects have the right to access, port, rectify, and erase data concerning their personal data (see the Reporters' Notes to Principles 21 to 23). While the GDPR's data rights are only granted to natural persons, some national data protection regimes also apply to legal persons (see Section 1 of the Austrian Data Protection Act (Datenschutzgesetz)). The current Council

Mandate on the E-Privacy Regulation (ST_6087_2021_INIT) is also intended to apply to end-users irrespective of whether they are natural or legal persons (ST_6087_2021_INIT, Article 1(2)). Being the subject of information, however, is not only a relevant factor in data protection law. For example, when a bank customer wants to make use of a third-party payment service provider, the customer may request that the bank make all the relevant account and transaction data available to the payment provider (Article 66 f. PSD II, Directive (EU) 2015/2366).

In the data ownership debate, it was suggested that data be assigned to the person who actually triggers its generation, the so-called "act of scripture" (see Thomas Hoeren, 'Dateneigentum – Versuch einer Anwendung von §303a StGB im Zivilrecht', 2013 *MultiMedia und Recht*, p. 486, 487). These Principles partly reflect this notion by taking into account the extent to which data was produced by a party's activities. That a party who owns and uses a product or service has a legitimate interest in the data produced by that activity is—at least to some extent—recognized by the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770). If a contract for the supply of a digital service/content is terminated, the trader shall refrain from using any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader (16(3) DCSD, Directive (EU) 2019/770; see the Reporters' Notes to Principle 21). Furthermore, Article 16(4) of the DCSD entitles the consumer to have the content retrieved that was created during the use of the digital service or content. Another example is Article 6(9) and 6(10) of the Digital Markets Act (ST 8722/2022 INIT), which obligate gatekeepers to provide effective portability of data generated through the activity of business and end users (see the Reporters' Notes to Principle 20). The European Commission considered assigning an exclusive "data producer's right" to the owner or long-term user of a device (COM(2017) 9 final, p. 13; Herbert Zech, 'Information as a tradable commodity', in: De Franceschi (ed.), *European Contract Law and the Digital Single Market*, 2016, p. 51 ff.), but ultimately discarded the idea of an exclusive right. Rather, the proposal for a Data Act assigns the user of an IoT device the (non-exclusive) rights to access and to share the data generated by its use with third parties (Articles 4 and 5 Data Act proposal).

That a party processing existing data in a way that adds value should have rights in the "new" data has similarities to the doctrines of production, combination, and commingling of tangible goods (for a comparative overview, see Brigitta Lurger and Wolfgang Faber, Principles for European Law - Study on a European Civil Code - Acquisition and Loss of Ownership in Goods, 2013, p. 1150 ff., 1180 ff.). "Production" is the process when a person, by contributing labor, produces new goods out of material owned by that or another person. The producer becomes owner of the new goods and the owner of the material is entitled, against the producer, to payment equal to the value of the material at the moment of production, secured by a proprietary security interest in the new goods (Article VIII.-5:201 DCFR; Article VIII.-5:201 Principles of European Law: Acquisition and Loss of Ownership of Goods (PEL Acq. Own.).) When goods owned by different persons are commingled in the sense that it is impossible or economically unreasonable to separate the resulting mass or mixture into its original constituents, but it is possible and economically reasonable to separate the mass or mixture into proportionate quantities, these persons become co-owners of the resulting mass or mixture, each for a share proportionate to the value of the respective part at the moment of commingling (Article VIII.-5:202 DCFR: Article

VIII.-5:202 PEL Acq. Own.). The rules on combination under Article VIII.-5:203 of the DCFR and Article VIII.-5:203 of the PEL Acq. Own. apply if goods owned by different persons are combined in the sense that separation would be impossible or economically unreasonable. If one of the parts is to be regarded as the principal part, the owner of that part normally acquires sole ownership of the whole, and the owner or owners of the subordinate parts are entitled, against the sole owner, to payment secured by a proprietary security interest in the combined goods. If none of the parts is to be regarded as the principal part, the owners of the component parts become co-owners of the whole, each for a share proportionate to the value of the respective part at the moment of combination.

Principle 19. General Factors Determining Rights in Co-Generated Data

(1) Data rights in co-generated data arise from considerations of fairness; accordingly, the way they are incorporated in existing legal frameworks under applicable law and the extent to which they may be waived or varied by agreement should be determined by the role such considerations of fairness play in the relevant legal system.

(2) In the case of co-generated data, a party that had a role in the generation of the data has a data right when it is appropriate under the facts and circumstances, which is determined by consideration of the following factors:

(a) the share that that party had in the generation of the relevant data, considering the factors listed in Principle 18;

(b) the weight of grounds such as those listed in Principles 20 to 23, which that party can put forward for being afforded the data right;

(c) the weight of any legitimate interests the controller or a third party may have in denying the data right;

(d) imbalance of bargaining power between the parties; and

(e) any public interest, including the interest to ensure fair and effective competition.

(3) The factors listed in paragraph (2) should also be taken into account for determining the specifications or restrictions of data rights, such as concerning data formats, timing, data security, further support required for exercise of the right to be fully effective, and remuneration to be paid.

Comment:

a. Relationship with existing legal frameworks. Paragraph (1) of this Principle describes the rights under Chapter B as reflecting considerations of fairness. This means that their implementation by courts or legislators should primarily occur within frameworks associated with fairness, which differ from jurisdiction to jurisdiction. In many legal systems, and in particular for cases in which there is a contractual relationship between the parties, implementation will occur by means of interpretation of the contract, applying doctrines such as unconscionability or principles such as good faith and fair dealing, or via rules that control unfair contract terms, when applicable. These Principles do not seek to indicate precisely how a jurisdiction should deal with the matter, leaving the matter to domestic law. A legislator may also implement Part III of these Principles as is, in which case a court might directly apply these Principles.

Illustration:

92. If a court is confronted with the question whether small airline A in Illustration no. 85 has a right against D to be provided access to the data, or a right against P that P arrange contractual relationships with its suppliers in a way that allows A to access the data, the court will do so within frameworks associated with fairness. As to the contract that A has with P, the court may—depending on the applicable law—solve the issue by way of contract interpretation according to good faith and fair dealing, or resort to doctrines such as that of contractual duties of care and consideration for the interests of the other party, unconscionability, or business-to-business unfair terms control. If the applicable law considers the relationship between A and M or D to be of a quasi-contractual nature that equally comes with enhanced duties of consideration for the interests of the other party, a court may use this tool. More generally, a court might, again depending on the applicable law, resort to laws and doctrines on unfair commercial practices, abuse of dominant market position, abuse of bargaining position, and the like.

Rights provided to a party under this Chapter may be waived or varied to the detriment of that party by agreement to the extent that such waiver or variation is allowed under the legal framework in which they are exercised. This means that the waivable or nonwaivable nature depends on the approach otherwise taken by the jurisdiction in which these Principles are implemented, and that a jurisdiction may in turn differentiate (e.g., treat transactions with consumers differently than business-to-business transactions). Accordingly, this Principle does not

propose a uniform concept of data rights. States that have a relatively strong tradition of private ordering (at least in business-to-business transactions) may choose to have many or all of the enumerated data rights treated as default rules, from which the parties may derogate by agreement. Other states, however, may treat some or all of the data rights as mandatory rules or, perhaps, as "sticky defaults" from which derogation is not impossible but is accompanied by procedural or substantive protections. For example, a jurisdiction that exercises strong control over unfair contractual clauses even in business-to-business relationships may, in line with that general policy, restrict waiver or variation of contract rules that might dilute that control. On the other hand, jurisdictions that place greater reliance on the role of private ordering (at least in nonconsumer transactions) in the creation of efficient transactions are more likely to treat the rules in this Part as default rules that are subject to contrary agreement of the parties. Even such jurisdictions, however, may afford less flexibility for such private ordering in the context of transactions in a regulated industry, such as the insurance industry.

b. Determining factors. These Principles identify five factors to be considered in determining whether it is appropriate to afford to a party a data right. These factors are listed in paragraph (2) of this Principle. They are: (a) the share that the party seeking access had in the generation of the relevant data, pursuant to the criteria set forth by Principle 18; (b) the weight of grounds such as those listed in Principles 20 to 23, which that party can put forward for being afforded the data right; (c) the weight of any legitimate interests the controller or a third party may have in denying the data right, considering Principles 20 to 23; (d) any imbalance of bargaining power between the parties; and (e) any public interest, including the interest to ensure fair and effective competition. It is to be noted that the competition aspect comes into play at various levels, and not only as a public interest: in particular, as far as the avoidance of lock-in effects is concerned, the ideal of fair and effective competition may coincide with private interests. Further, public interests may both be an argument for and against granting access, so the fifth criterion works in both ways.

The factors listed in paragraph (2) of this Principle are not ordered by their relative weight, but should be balanced against one another in a flexible manner. This means that if the ground a party brings forward, e.g., under Principle 20, has particular weight, it may compensate for a relatively insignificant contribution to data generation. Such flexibility is also necessary in order to enable these Principles to be implemented by different legal frameworks, ranging from contract law, to specific statutory regimes (horizontal or sectoral), to competition law, depending on the

relevant jurisdiction. Depending on the legal framework chosen by a jurisdiction to implement these Principles, it is even possible that a factor listed in this Principle might be reduced to a degree of weight that is almost negligible.

c. Choice of factors. As to the share a party had in the generation of the data, see the Comments to Principle 18. As to the weight of grounds that that party can put forward for being afforded the data right, see the Comments to Principles 20 to 23. Legitimate interests in denying the data right are, for instance, data protection or trade secret concerns.

Imbalance of bargaining power is a standard justification for legal systems to interfere with private ordering for the protection of vulnerable groups, such as consumers, employees, tenants, or authors with regard to their works. In competition or antitrust law, the idea appears both in the guise of dominant market position in terms of a market share and, depending on the relevant jurisdiction, of dominant position within a bilateral relationship. In some jurisdictions, there are an increasing number of specific protective regimes for the benefit also of smaller businesses confronted with bigger businesses, such as for small-to-medium-sized enterprises' marketing products or services via a platform. When contract law allows for the assessment of the fairness of an agreement, any imbalance in bargaining power is an important argument that a court may take into account when assessing the deal. Paragraph (2)(d) of this Principle may cover all of these scenarios, but is not intended to create any new form of "pseudo-competition law." Rather, jurisdictions will implement this Principle in a legal framework that fits into the general legal landscape and does not cause any disruptive effects.

The relevance of the public interest within private relationships, in particular between businesses, is normally very low, while it is the predominant idea underlying the data rights addressed in Principles 24 to 27. However, public interests, such as the interest in ensuring fair and undistorted competition, are always present to some extent, and when a state decides to implement these Principles within its competition law, for instance, they may already be seen as a justification for data rights from very different point of views.

d. Specifications. A court or legislator grappling with co-generated data usually has at least two decisions to make: First, whether to grant a data right, and second, how this right must be granted, i.e., what are the modalities with regard to formats, timing, and the like, and whether access must be provided for free or in return for appropriate remuneration. In taking the latter decision, a court or legislator will have to consider, among other factors, the type and weight of the parties' respective shares in the generation of the data (e.g., when a share involved considerable monetary

investment, this may be an argument against giving the other party a free ride) and the efforts required for complying with the right. In assessing what is appropriate in the circumstances, the factors listed in paragraph (2) have to be taken into account.

REPORTERS' NOTES

United States:

See the Reporters' Notes to Principle 18.

Europe:

a. Relationship with existing legal frameworks. There are different ways that data rights in co-generated data can be implemented. Until now, the European legislator has introduced data rights largely independently of a contractual relationship between the parties; for example, in Articles 16 to 20 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), or in Articles 6(9) and (10) Digital Markets Act (DMA) (Regulation (EU) 2022/1925). However, with the proposal for a Data Act (COM(2022) 68 final), the European Commission has just put forward a new approach that clearly relies on a contractual relationship with the "data holder." The proposal entitles users of "Internet of Things" (IoT) products and related services to access and share the data generated by the use of those products or services (Articles 4 and 5 Data Act proposal), and introduces an unfairness test for contractual terms regarding the access and use of data that have unilaterally been imposed on micro-, small-, and medium-sized enterprises (MSMEs) (Article 13 Data Act proposal). However, and as already set out in these Principles, there will not always be a contractual relationship between the party seeking a data right and the data holder. The European Commission's current approach is to overcome this issue by setting out that the data holder may only use non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user (Article 4(6) Data Act proposal). Whether this approach will be adopted by the European co-legislators remains to be seen.

b. Determining factors. The factors listed in this Principle are also considered relevant by the German Data Protection Commission when deciding whether to grant a data right (see Opinion of the German Data Ethics Commission, 2019, p. 85 f.). A similar set of factors that has been proposed includes: (1) establishing a functioning and competitive market for the data economy; (2) promoting innovation; (3) protecting consumer interests with a particular focus on protecting the privacy of natural persons; and (4) promoting additional public interests (Josef Drexl, Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy, in Reiner Schulze and Alberto De Franceschi (eds.), Digital Revolution – New Challenges for Law, 2019, p. 11 ff.; id, Data Access and control in the area of connected devices, 2018, p. 51 ff.).

With regard to the significance of the share a party had in the generation of data, see the Reporters' Notes to Principle 18. With regard to the grounds that a party relying on a data right can put forward for being afforded that data right and the possible legitimate interests of the controller or third party, see the Reporters' Notes to Principles 20 to 23.

A party's relative bargaining power is a standard criterion underlying much of the mandatory rules or "sticky" default rules enshrined in legal systems in Europe. This certainly holds true for the whole of consumer law, the introduction of which is justified, to a major extent, by the consumer's relative weakness in bargaining power. Similar considerations have led to the introduction of protective mechanisms for employees or tenants of residential premises. More recently, and also with regard to co-generated data, the Platform to Business Regulation (P2B) (Regulation (EU) 2019/1150) has introduced some minimum rights for small and medium enterprises (SMEs) whose bargaining position vis-à-vis a platform provider is usually very weak. Moreover, the Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain (Directive (EU) 2019/633) prohibits practices that deviate from good commercial conduct in the agricultural sector if the supplier has a lower annual turnover than the buyer, and thus aims to address significant imbalances in bargaining power. Considerations of imbalance in bargaining power have also visibly guided the policy decisions taken in the Data Act proposal. The most obvious example is the unfairness test for contract terms concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations (Article 13 Data Act proposal). Micro-, small-, or medium-sized enterprises (MSME) must be protected against contractual terms that have been unilaterally imposed on them and that prevent or limit the use of data to the generation of which the MSME contributed. According to Article 13(6) of the Data Act proposal, a contractual term is considered "unilaterally imposed" if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. When looking at the Recitals, it becomes clear that the data access and sharing rights afforded to users of "Internet of Things" (IoT) products (Articles 4 and 5 Data Act proposal) should also address situations of unequal bargaining power. Recital 19 of the Data Act proposal states that there is an imbalance in bargaining power between the user and the data holder because IoT products are often designed in a way that the data can only be accessed by the data holder and the users are unable to obtain any access to the data. An imbalance between the controller and the data subject also has to be considered when determining whether consent is freely given under the GDPR (see Recital 43 GDPR). Also, EU competition law is, to a large extent, based on the idea that unequal bargaining power, which may arise with regard to a particular relationship (such as a supplier–customer relationship) or more generally because of a dominant market position, may justify corrective mechanisms, including access and similar rights.

Public interests are widely recognized as justification for data sharing obligations, which is now also reflected by the Data Act proposal, which intends to remove barriers to data sharing in order to achieve a well-functioning internal market for data and ensure an allocation of data that benefits society overall (see Recitals 2 and 4 Data Act proposal). But public interests may also justify data rights beyond co-generation (see the Reporters' Notes to Principle 24). For example, data sharing under the Clinical Trial Regulation is justified by the protection of public health and the fostering of the innovation capacity of European medical research (see Recital 67 Regulation (EU) No 536/2014). Data sharing under the Markets in Financial Instruments Regulation (MiFIR) serves the protection of the financial market (cf. Recitals 14 et seq. Regulation (EU) No 600/2014), and sharing of information under the Road Safety Regulation serves the safety of road traffic (Commission Delegated Regulation (EU) No 886/2013). The justification for data sharing under

the Infrastructure for Spatial Information in the European Community (INSPIRE) Directive (cf. Recital 1 Directive 2007/2/EC) is environmental protection and mandatory data sharing under the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation (Regulation (EC) No 1907/2006) serves public interests of avoiding unnecessary testing on vertebrate animals.

d. Specifications. The factors set out by this Principle not only provide guidance on whether to create a data right but also on how to implement it. The specifications of existing data rights in European law vary to a large extent, which may best be illustrated by comparing the various access/portability rights (for a detailed analysis, see Inge Graef, Martin Husovec and Jasper van den Boom, 'Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes' [2020] Journal of European Consumer and Market Law 3). For example, the GDPR's data portability right may be exercised free of charge unless the requests are "manifestly unfounded or excessive, in particular because of their repetitive character." In the latter case, the controller can charge a reasonable fee or refuse to act (Article 12(5) GDPR). Under the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770), the consumer may retrieve any content, other than personal data, that was provided or created by the consumer when using the digital content or digital service free of charge (Article 16(4) DCSD). In comparison, the Payment Sector Directive II (PSD II) (Directive (EU) 2015/2366) does not require banks to grant payment service providers access to account information free of charge, but merely stipulates that the bank must not discriminate against any payment service providers (Article 66(4) PSD II). The right to access and share data under the Data Act proposal must be free of charge to the users (Articles 4(1) and 5(1)). Granting access to the data free of charge is also stipulated in Article 6(10) of the Digital Markets Act (DMA) (Regulation (EU) 2022/1925).

The notion that unequal bargaining power must also be taken into account as a factor when determining the specifications of data rights is reflected in Article 9 of the Data Act Proposal. If the user exercises its rights to have data transferred to a third-party recipient, the recipient and the data holder may agree on compensation that must be reasonable (Article 9(1)). However, if the recipient is an MSME, the compensation must not exceed the costs directly related to making the data available to the data recipient and that are attributable to the request (Article 9(2)).

The rights under the DCSD and the GDPR have to be fulfilled within a reasonable time (Article 16(4) DCSD) or without undue delay, and in any event within one month of receipt of the request, but that period can be extended to two months when necessary (Article 12(3) GDPR). Fulfilment periods of up to two months would, of course, be incompatible with the requirements of payment services, which require real-time access in order to provide a timely transfer. Thus, Article 66(4)(b) of the PSD II provides that the relevant data needs to be made available immediately after the receipt of a payment order. The same holds true for the rights to access and share under the Data Act proposal, which have to be fulfilled without undue delay (Article 4(1) and 5(1) Data Act proposal).

Regarding the format of the data, Article 20 of the GDPR sets out that the data subject has the right to receive the data in "a structured, commonly used and machine-readable format." Hence, the appropriate format may depend on the specific sector (Article 29 Working Party, Guidelines

on the right to data portability (2017) WP 242 rev.01, 17). That the PSD II does not specify or delegate the standardization of application programming interfaces (APIs) is seen as a major shortcoming of the instrument and its access right (see European Commission, Retail Payments Strategy for the EU, COM(2020) 592 final). Standardization efforts in the banking sector are pursued by industry led initiatives (see Berlin Group, NextGenPSD2). While under Article 20 of the GDPR the data is only supplied on a one-off basis, Article 6(9) and 6(10) of the Digital Markets Act (DMA) and Articles 4(1) and 5(1) of the Data Act proposal set out that access be provided continuously and in real-time.

Principle 20. Access or Porting with regard to Co-Generated Data

(1) Grounds that, subject to Principle 19, may give rise to a right to access or to port co-generated data include circumstances in which the access or porting is:

(a) necessary for normal use, maintenance, or resale by the user of a product or service consistent with its purpose, and the controller is part of the supply network and can reasonably be expected to have foreseen this necessity;

(b) necessary for quality monitoring or improvement by the supplier of a product or service consistent with duties of that supplier, and the controller is part of the supply network and can reasonably be expected to have foreseen this necessity;

(c) necessary for establishing facts, such as for better understanding by a party of that party's own operations, including any proof of such operations that party needs to give vis-à-vis a third party, when this is urgently needed by that party and the access to or porting of the co-generated data cannot reasonably be expected to harm the controller's interests;

(d) necessary for the development of a new product or service by a party when such development was, in light of that party's and the controller's previous business operations, the type of their respective contributions to the generation of the data, and the nature of their relationship, to be seen primarily as a business opportunity of that first party; or

(e) necessary for the avoidance of anti-competitive lock-in effects to the detriment of a party, such as by preventing that party from rightfully switching suppliers of products or services or attracting further customers.

(2) Consistent with Principle 19(3), a right under paragraph (1) should be afforded only with appropriate restrictions such as disclosure to a trusted third party, disaggregation,

anonymization, or blurring of data, to the extent that affording the right without such restrictions would be incompatible with the rights of others, or with public interests.

(3) The controller must comply with the duties under Principle 32 for the protection of third parties, and restrictions under paragraph (2) must in any case enable the controller to do so.

Comment:

a. General observations on access rights. In practice, access rights and related rights are the most important data rights to be exercised vis-à-vis a controller in the data economy. Access to data is of utmost importance for players to be able to understand better and to improve their own business operations, to develop new products and services, to have a better choice between different suppliers, and for many other purposes. Simple access to the data is sometimes insufficient for satisfying the legitimate interests of the party relying on the right, and transfer of data to that party or a third party may be required as well. This Principle focuses on spelling out in greater detail what a legitimate ground is on which the party seeking access may rely. Paragraph (1) lists some typical situations in which a party has a legitimate interest in obtaining access to data or in having it ported. This list is not meant to be exhaustive.

This Principle may be decisive for a legislator or court for affording to a particular party who has contributed to the generation of data a right to have access to data or to port data, as well as for parties when negotiating an agreement or for standardization agencies and similar bodies when defining best practices. A court could make use of this Principle, for example, when applying the unconscionability or unfairness test to contract clauses that are subject to such a test.

b. User-generated data. An issue that has been troubling parties in the data economy, courts, and legislators alike is the issue of a user's right to access user-generated data, i.e., data generated by the user through the use of a product or service. The relationship between a user and a controller of user-generated data raises a wide range of complex legal issues. Often, the customer is in the weaker position because it is in need of the commodity supplied, has already paid the full purchase price to the supplier, and did not focus on the issue of data rights at the time of the purchase. This is shown in the following Illustration.

Illustration:

93. Farm corporation F buys from seller S a "smart" tractor manufactured by manufacturer T. The tractor's operating software is set up so that F will not be able to use

the tractor unless, when initializing it, F accepts and enters into end user agreements with T and businesses U and V acting in cooperation with T. The end user agreements are about licenses to use embedded software and software to be downloaded on a mobile telephone, and about digital services to be provided to F, including weather forecasts, soil analyses, targeted recommendations concerning the use of particular fertilizers and insecticides, and predictive maintenance. If anything goes wrong with these licenses or services, F is in a weak position, having paid the full purchase price to S who will, under many legal systems, not be responsible for what T, U, and V are doing, or be responsible only during a very short period after delivery.

As it is mainly within the discretion of the supplier (or producer) to what extent data that is absolutely necessary for the use of the commodity will be stored in external locations outside the sphere of control of the customer, the customer becomes increasingly dependent on the continuing goodwill of controllers. This is why customers should, in certain cases, at least have a right to obtain access to their user-generated data. A typical situation in which this is justified is when normal use of the relevant commodity by the customer, including any necessary repair, requires access to the data. In such a case, the customer should have the right to obtain access to the data, or to designate a person to whom access is given. This ground overlaps to a certain extent with the ground of avoidance of lock-in effects.

Illustration:

94. The tractor of farm corporation F in Illustration no. 93 is damaged in an accident. Manufacturer T's authorized repair shop states the tractor cannot be repaired, and recommends that F buy a new tractor. F would like to have a second opinion from an independent repair shop, but the independent repair shop cannot evaluate whether the tractor can be repaired without access to data about the tractor held by T. F should be able to access the data or designate the independent repair shop as a party to be given access.

Suppliers of connected commodities can also control the resale of the commodities even when the law would normally not allow them to do so. Under the current law, control of redistribution may be rightful, at least to a certain extent, in the realm of copyright protected works, but usually not when ordinary tangible property is supplied in return for a purchase price. When the customer is allowed to resell, the controller of user-generated data should not be allowed to

discourage or prevent the customer from reselling by withholding user-generated data or in similar ways. Rather, the customer may have a right against the controller to take all necessary steps in order to put a third-party buyer in the same position as the customer. This follows from Principle 19(3), according to which access rights may have to be afforded further support for exercise of the right to be fully effective.

Illustration:

95. Farm corporation F in Illustration no. 93 wants to resell the tractor to G. However, if the transaction is to make sense in economic terms, resale of the tractor would require that G be able to utilize all the data accumulated by F's use of the tractor. In order to do so, G would also need further support, such as the ability to use software and digital services that came with the tractor. F has a right to require T to take all necessary steps in order to achieve this goal.

c. Supplier-generated data. With the "Internet of Things" (IoT), every step in a value chain potentially generates data, and this data may be a valuable asset to more than just the party in the value chain that happens to have collected and to control the data. A common situation in which this is the case and there is a particularly strong ground for requiring access to data is when a supplier, e.g., of components, needs access for the purpose of quality monitoring and improvement consistent with its duties. This is particularly relevant when there is no direct contractual link between the parties but when both parties are links in a supply chain or supply network.

Illustration:

96. Company M produces motors for the tractors manufactured by T in Illustration no. 93. Data concerning motor performance is collected, but not directly by T. Instead, V, one of the cloud service providers cooperating with T, controls the motor data. M needs access to the motor data in order to ensure the motors work as promised, in particular as M has agreed to liability for losses that occur if motor problems exceed a particular threshold. In this situation, M has a legitimate ground for obtaining access to the motor data.

d. Establishing facts. Frequently, the interest of the party seeking access to the data has nothing to do with the value chain or value network in which that party and the controller are involved. Rather, the party urgently needs access for establishing facts, such as for a better understanding of its own business operations, or in litigation with a third party (to the extent this

is not already dealt with under procedural law in the relevant jurisdiction), and that access could not possibly harm any interests of the controller. Again, this may constitute a legitimate ground.

Illustrations:

97. F in Illustration no. 93 sold a piece of land to third party D, and now D is suing F for an alleged breach of a warranty. F would need data controlled by T to be able to prove, in the litigation between F and D, that the soil was of a particular quality when D took over the land from F. In this scenario, F has a significant share in the generation of the data, F is urgently in need of the data, and providing the relevant dataset to F cannot reasonably harm T's legitimate interests provided the dataset is limited and does not imply disclosure of any of T's trade secrets.

98. B runs a shopping-rewards plan under which customers shopping with particular retailers earn reward points. Customer data is collected by B and used for customer profiling and targeted advertising. C, who has just paid in cash at the shop of retailer R and had the reward points credited to his account, is accused of shoplifting and arrested by the police. C can prove his innocence by demonstrating that the purchase was registered on the reward account and that he must therefore have paid for the goods. In this case, very strong factors would weigh in favor of an access right on the part of C, C having generated the information, being the subject of the information, and being urgently in need of the data.

e. Development of smart products or services. Much of the data economy relies on the development of innovative smart products or services. There are often several parties that would, in principle, be in a position and willing to develop such products and services, and they may be competing with each other. Such competition is normally good for innovation. However, sometimes a party uses its position and bargaining power to monopolize huge amounts of data, fencing off other businesses that may be as well-equipped, or even much better equipped, to exploit the data's economic potential. Normally, the parties will enter into negotiations and transactions and make a deal that leads to efficient outcomes, but sometimes this is not the case, e.g., because one party abuses its dominant bargaining position.

Illustration:

99. M in Illustration no. 96 is the company that produces the motors for the tractors produced by T. Data concerning motor performance on the road is stored by V, a provider of cloud navigation services that cooperates with T. M would like to develop a predictive maintenance service and would need access to the motor performance data for this purpose. However, V refuses to give M access because V and T together plan to start their own motor predictive maintenance service as a new field of business. In this situation, consideration must be given to the fact that M is a motor company (and V is not), that predictive maintenance is being developed with regard to motors produced by M (and not by V), that M's contribution to the generation of the data is very significant (while V's contribution is, in the first place, to just collect the data), and that V is simply a service provider who should normally not be using such data for its own purposes anyway. In light of these circumstances, developing predictive maintenance services for its own motors with the help of the data appears to be a business opportunity primarily for M. M may thus, subject to the other factors mentioned in Principle 19, have an access right against V. This access right of M is without prejudice to the possibility that M may even have a right against V to require V to desist from such data use.

f. Prevention of lock-in effects. User-generated data has huge potential to create "lock-in" effects, e.g., the more user-generated data has been accumulated by a particular controller, the more difficult it becomes for the user to switch the supplier of a product or service. Suppliers sometimes exploit this effect by strategic and often anti-competitive behavior, such as by raising the price of commodities once the supplier has accumulated enough user-generated data for the customer to be effectively "locked in." From an economic perspective, this is an undesirable situation, which is also likely to harm the customer's legitimate interests. This is why this Principle may provide the customer a right of access to the user-generated data or the right to have it transmitted to another party.

Illustrations:

100. Farm corporation F in Illustration no. 93 wants to buy a new tractor. As tractors manufactured by T have become very expensive F decides to buy a similar, but less expensive, tractor manufactured by U. However, in order to take full advantage of the functionalities of this kind of tractor, including a variety of analytical tools based on data

collected from the same parcel of land in the past, F would need access to data about that parcel of land controlled by T. Unless F has a right against T to have this data transferred to U, F is "locked-in" and may effectively be prevented from switching manufacturers, which would be both harmful to F and to farmers and competition at large. Therefore, F has a right to access to the data collected by the tractor.

101. Small business S markets goods over the online marketplace run by platform provider P. Over the years, S has accumulated a bulk of very positive evaluations by customers, expressed as 4.8 out of 5 possible credit "stars" and many enthusiastic feedback messages. When S seeks to move to another online marketplace (run by Q), S requests to have the reputational data transferred to Q. In determining whether S has rights against P to have the reputational data transferred, a court should take into account, inter alia, that S has worked hard over many years to produce the information coded in the data, that S is in need of the data for a legitimate interest, and that denying portability of reputational data has anti-competitive effects.

Similar considerations may apply when a supplier needs access to data in order to be able to attract further customers apart from the controller, i.e., lock-in situations do not only occur with regard to users.

g. Restrictions. Paragraph (2) clarifies that, consistent with Principle 19(3), restrictions on rights to access or port co-generated data may have to be imposed in order to protect legitimate interests on the part of the controller or third parties. This means that a data right vis-à-vis the controller is afforded only with appropriate restrictions such as anonymization or disclosure to a trusted third party.

Illustration:

102. M in Illustration no. 96, the company that produces the motors for the tractors produced by T, requests access to the motor data held by cloud service provider V. However, some of the motor data is data relating to identifiable natural persons within the European Union and is, at least potentially, subject to EU data protection law. In this case, a court will afford the access right subject to appropriate safeguards and make sure M bears the costs.

This is particularly important as paragraph (3) clarifies that the controller must comply with the obligations under Principle 32 with regard to the protection of third parties. There might theoretically indeed be a clash between the fact that a controller is faced on the one hand with a data access right and on the other hand with an obligation to exercise due diligence and take reasonable and appropriate steps for the protection of third parties under Part IV, Chapter A. As a first step, third parties' rights had already been taken into account when weighing different factors and deciding whether or not to afford the access right, cf. Principle 19(2)(c). If the outcome of this is that the access right should be afforded, the second step is to determine the exact conditions, such as concerning data formats or remuneration and other modalities under Principle 19(3) and, more specifically, concerning third-party protection under paragraph (2) of this Principle. In doing so, a result must be achieved that avoids any clash or inconsistency between the controller's obligation to grant access and obligation to comply with the duties under Principle 32. This is to be achieved by way of legal, technical, and/or institutional safeguards.

Illustration:

103. In Illustration no. 102 there could be a contract between M and V that imposes strict obligations on M for the protection of the data subjects, including that data access and processing is only allowed for a limited number of purposes. V could then grant access to M in a secure environment controlled by V or T, with V or T monitoring processing activities by M in that environment and making sure no data that might cause harm to the data subjects leaves the environment.

REPORTERS' NOTES

United States:

Data porting rights are addressed extensively in Principles of the Law, Data Privacy § 9 (AM. L. INST. 2020), particularly in the context of user-generated data. As stated in Comment *a* to that Section:

> Data portability permits a data subject to control his or her personal information and can also further consumer choice among enterprises. If a data subject is not able to leave a service or platform with his or her personal data, he or she may be "locked in" to it. The result can be highly negative for the development of a "market" for privacy and security, in which entities compete to develop pro-privacy terms of service and increase their security standards. Data portability also helps safeguard personal information when a legacy provider goes out of business.

Perhaps the broadest U.S. statute providing for data portability is the California Consumer Privacy Act of 2018. Section 1798.100(d) of that Act provides that:

> A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

CAL. CIV. CODE § 1798.100(d).

In addition, there are quite a few precedents for sector-specific data portability rights in the United States. These rights are addressed in some detail in the Reporters' Notes to Principles of the Law, Data Privacy § 9 (AM. L. INST. 2020), which should be consulted in this regard. Examples provided there include telephone number portability (see Communications Act of 1934, as amended, 47 U.S.C. §§ 251(b)(2) and 153(37); 47 C.F.R. § 52.21(n)) and health information within the scope of the Health Insurance Portability and Accountability Act (HIPAA) (see 45 C.F.R. § 164.524). With respect to electronic medical records, see Health Information Technology for Economic and Clinical Health Act (HITECH Act), 42 U.S.C.A. § 17935(e)(1) (providing that "[I]n the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual . . . the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific.").

Europe:

For personal data, the most prominent example of a portability right in Europe is Article 20 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Under that provision, data subjects have the right to receive the personal data concerning them, which they provided to a controller on the basis of consent or of a contract, in a structured, commonly used, and machine-readable format, and have the right to transmit those data to another controller without hindrance, and even to have the personal data transmitted directly from one controller to another, when technically feasible. The objective of data portability is to enhance the data subject's control over his or her data (Recital 68 GDPR) and to prevent "lock-in" by enabling the data subject to switch providers (Article 29 Data Protection Working Party, Guidelines on the right to "data portability", wp 242 rev.01, p. 5). Article 20 GDPR is based on considerations of facilitating the free flow of data rather than data protection, which is underlined by the fact that exercising the right does not require the initial data holder to erase the data.

With the Data Act proposal (COM(2022) 68 final), the European Commission has put forward a number of provisions that reflect the idea that a party that contributed to the generation of data has a right to access and use that data. Article 4(1) obliges data holders to make available

to the user of an "Internet of Things" (IoT) product or related service the data generated by its use of that product or service. Furthermore, at the user's request, data holders have to make available the data generated by the use of an IoT product or related service to a third party (Article 5(1)). While the Data Act proposal does not specify any grounds on which the user seeking access needs to rely, the access and sharing rights are, just like this Principle, based on considerations of fairness, and take into account the legitimate interests of the data holder and third parties. Articles 4(1) and 5(1) generally grant the user the right to access and share all the data generated by the use of an IoT product or related service. However, to protect trade secrets of the data holder and third parties, Article 4(3) of the Data Act proposal stipulates that trade secrets shall only be disclosed provided that all specific, necessary measures are taken to preserve the confidentiality of trade secrets, in particular with respect to third parties. In case the data is shared with a third-party recipient, Article 5(8) contains similar obligations. In addition, the Data Act proposal prohibits any use of the obtained data for the development of a product that competes with the product from which the data originate (Articles 4(4) and 6(2)(e)). Third-party recipients are also prohibited from making the obtained data available to another third party, in raw, aggregated, or derived form, unless necessary to provide the service requested by the user (Article 6(2)(c)).

Article 13 of the Data Act proposal provides for an unfairness control of contractual terms unilaterally imposed on a micro-, small-, or medium-sized enterprise (MSME) (Article 13 Data Act proposal), which is also intended to address the issue of denied or limited access to co-generated data. A contract term is presumed unfair if it prevents an MSME from using the data contributed or generated by the MSME during the period of the contract, or limits the use of such data to the extent that the MSME is not entitled to use, capture, access, or control such data, or exploit the value of such data in a proportionate manner (Article 13(4)(c)). A contractual term that prevents an MSME from obtaining a copy of the data, which was either generated by the MSME or to which it contributed, during the period of the contract or within a reasonable period after the termination thereof is also presumed unfair (Article 13(4)(d)). Because contract terms of this sort are on the grey list (they are only presumed unfair), the Data Act proposal leaves courts enough leeway to balance the interests of the MSME against those of the contractual partner/data holder and any third parties.

Data access and portability obligations, based on considerations of co-generation, have also been enshrined in the Digital Markets Act (DMA) (Regulation (EU) 2022/1925). In Article 6(9), the Regulation obligates gatekeepers to provide end users effective portability of the data they provided or generated in the context of their use of the relevant core platform services of the gatekeeper, in a structured, commonly used, and machine-readable format. This should enable the end users to port that data in real time effectively and thus facilitate switching or multi-homing. In addition, Article 6(10) of the DMA obligates the gatekeepers to grant business users, free of charge, effective, high-quality, continuous, and real-time access and use of data provided or generated by the business users while using the relevant core platform services and also data inferred from the provided and generated data (see Recital 60 DMA). This also applies to data provided or generated by end users engaging with the products or services provided by those business users.

If a consumer terminates a contract for the supply of digital content or a digital service due to lack of conformity, the Digital Content and Services Directive (DCSD) (Directive (EU)

2019/770) affords the consumer a data portability right for non-personal data: According to Article 16(4) of the DCSD, the consumer has, in the event of termination, the right to request from the trader any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader. The rationale of the rule is partly the rationale of restitution after the termination of a contract, and partly reduction of lock-in effects as consumers might be discouraged from exercising their right to terminate the contract if they would be deprived of access to the content they created by using the digital content or service (Recital 70 DCSD). However, the provision does not create any additional obligation of the trader to retain data generated under a contract (cf. the initial formulation in Recital 39 of the Commission Proposal (COM(2015) 634 final), which indicated such an obligation).

Data access/portability rights can also be found in sectoral regimes. In the banking sector, the Payment Sector Directive II (PSD II) (Directive (EU) 2015/2366) gives payers the right to allow third-party providers to access their account information held by the payer's bank in order to provide payment initiation or account information services (Articles 66 f). This so-called "access-to-account" rule is based on the rationale that payers should be able to use innovative financial technology ("fintech") services without being dependent on the willingness of established banks to grant access to the data that is necessary to perform such services. Since these third-party providers are likely to compete with established banks for a lucrative line of business in the financial sector, the banks have an incentive to forestall competition by denying access to the data required to offer the competing services, depriving payers of new payment services. The payer, who co-generated the account data (see Principle 19), is the person exercising the access/portability right and is also the primary beneficiary of the right. However, the payment service providers are, of course, indirect beneficiaries of the access-to-account rule.

A data access right in the context of maintenance of assets is provided by Articles 61 ff. Type Approval Regulation (Regulation (EU) 2018/858), which requires vehicle manufacturers to provide to independent operators unrestricted, standardized, and non-discriminatory access to vehicle on-board-diagnostics (OBD) information, etc. However, there is a conceptual difference between rights described above, in particular in the PSD II, and the access right under the Type Approval Regulation, as the latter is assigned to independent repair service providers, who have not contributed to the generation of the data. The car owners, who have a share in the generation of—at least most of—the data are only the indirect beneficiaries of the rule. Hence, Article 66 ff. of the Type Approval Regulation would, under these Principles, rather qualify as a data right for the public interest (see Chapter C); the public interest being a functioning aftermarket in the automobile sector. It is in a similar vein that several Implementing Regulations of the European Commission based on the Ecodesign Directive oblige the manufacturer, importer, or authorized representative to provide access to repair and maintenance information of certain products (e.g., household washing machines, see Annex II 8(3) of Commission Regulation (EU) 2019/2023, or refrigerating appliances with a direct sales function, see Annex II 2(c) of Commission Regulation (EU) 2019/2024).

Porting of data is also one of the essential elements of the Free Flow of Data Regulation (Regulation (EU) 2018/1807). That Regulation applies to the porting of non-personal data in business-to-business (B2B) relationships, and encourages the Commission to contribute to the

development of EU-wide codes of conduct to facilitate the porting of (non-personal) data in a structured, commonly used, and machine-readable format, including open standard formats (Article 6). On this basis, the Switching Cloud Providers and Porting Data (SWIPO) Working Group, which is one of the Digital Single Market Cloud Stakeholders Working Groups gathering more than 100 stakeholders, adopted in November 2019 two draft Codes of Conduct. The first one is on infrastructure as a service market and the second one on software as a service market. These Codes of Conduct will be assessed by the Commission by the end of 2022 (Article 8 Regulation (EU) 2018/1807).

Article 9 of the Platform to Business Regulation (P2B) (Regulation (EU) 2019/1150) obligates the providers of online platforms to disclose to business users the extent to which they will be granted access to data (such as customer data). Initially, the European Parliament's Committee on Transport and Tourism proposed to grant commercial platform users a right to access all data collected by the platform operators "on the basis of the commercial activity of the respective business user" (Amendment 58 of Opinion of the Committee on Transport and Tourism, COM(2018)0238 – C8-0165/2018 – 2018/0112(COD)). However, the final provision is limited to a mere transparency requirement. The ELI Model Rules on Online Platforms go one step further and call for a right to port reputational data (Article 7: Portability of Reviews).

Principle 21. Desistance from Data Activities with regard to Co-Generated Data

Grounds that, subject to Principle 19, may give rise to a party's right to require that the controller desist from data activities with regard to co-generated data, up to a right to require erasure of data, should include situations in which:

(a) the data activities cause, or can reasonably be expected to cause, significant harm, including non-economic harm, to that party; and

(b) the purpose of the data activities is inconsistent with the way that party contributed to the generation of the data, in particular because

(i) that party was induced to contribute to the generation of the data for an entirely different purpose and could not reasonably have been expected to contribute to the generation of the data if it had known or foreseen the purpose of the data activities engaged in by the controller; or

(ii) that party's assent to its contribution to the generation of the data for that purpose was obtained in a manner that is incompatible with doctrines that vindicate important public policies including those that protect parties from overreaching conduct or agreements.

Comment:

a. General observations on desistance. While access rights within the meaning of Principle 20 may be the most important type of data right, there are also cases in which it may be justified to afford to a party a right to require that the controller desist from a particular use of data that party has co-generated. Whether it is appropriate under the facts and circumstances to provide a party with such a right is determined by consideration of the factors listed in Principle 19. This Principle explains in more detail what should count as a legitimate interest or ground for requiring a controller of data to desist from using co-generated data (and, in some cases, to erase it).

b. Grounds to be put forward for desistance. Grounds that may give rise to a party's right to require that the controller desist from data activities with regard to co-generated data include situations in which the activities are causing significant harm, including non-economic harm, to that party when the controller's purpose of use is inconsistent with the purpose for which that party was induced to contribute to the generation of the data and that party could not reasonably have been expected to contribute to the generation of the data if it had known or foreseen the purpose of use by the controller. In order to make this judgment, and unless there are any indications that the individual party concerned had different priorities and preferences, an objective test should be applied by default. The judgment should be based on the assumption that there is effective competition and that the relevant party had a choice.

Illustrations:

104. Manufacturer T of the smart tractor in Illustration no. 93 uses the data collected by the tractor to create a database that can be sold to potential buyers of farmland, providing extensive details about soil quality, in order to enable such potential buyers to make a more informed decision regarding the price they would be willing to pay for the land. The availability of this data would cause significant harm to F because such potential buyers would have better information about the soil quality than F itself. F has contributed to the generation of the data for an entirely different purpose (i.e., in order to benefit from precision farming services), disclosing the data to buyers of land is inconsistent with that purpose, and a person in F's position would not reasonably be expected to produce the data if the person had known how T would make use of the data. F has a legitimate ground to require that T desist from making the data available to potential buyers.

105. Company X runs a social network. In contracting to use that social network, individual Y expressly agrees, in the privacy statement, that X may use Y's photos and personal contacts for any purpose X deems fit, including for profiling. X feeds all photos and personal contacts into a database that is analyzed by artificial intelligence to create a profile of Y. Employers are prepared to pay high prices for job candidates' profiles. Because Y had uploaded several photos that show him drunk at parties, and this information is revealed by his profile, potential employers who bought access to Y's profile declined to offer Y a job on various occasions when, in the absence of the profile information, the job would have been offered to Y. Y would not have agreed to the contract with the social network had Y understood what might be implied by "profiling." Y therefore has grounds to require that X desist from disseminating his profile.

There may also be cases in which a party has given, or would have given, consent, e.g., due to particular weaknesses or preferences, but obtaining that consent was incompatible with doctrines that vindicate important public policies or those that protect parties from overreaching conduct or agreements. Such public policies differ from jurisdiction to jurisdiction.

Illustration:

106. Assume that individual I in Illustration no. 105 was a young person with a very positive attitude toward anything digital and a "sharing is caring" philosophy. Assume further that I was aware that any photos he might upload could become part of his profile accessible to some potential future employers, but took the position that he would not like to work for people who do not "share his lifestyle." Even if, 10 years later, I is no longer comfortable with the fact that potential employers can have access to his profile that reveals embarrassing activities from I's younger days, the test under subparagraph (b)(i) of this Principle would not be fulfilled. However, subparagraph (b)(ii) of this Principle might still apply if instigating a young person to risk their future career is held to be incompatible with public policy under applicable law.

REPORTERS' NOTES

United States:

See Principles of the Law, Data Privacy § 7(a) (AM. L. INST. 2020): "Personal data shall not be used in secondary data activities unrelated to those stated in the notice required by Principle 4 without a data subject's consent." As stated in Comment *a* to that Section, "The concept of

relevancy of personal data for the initial purpose and further processing means that data shall be tied to the initial use and not used for unrelated purposes." Id., Comment *a*.

See also the California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100(a) ("A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.").

As pointed out in the Reporters' Notes to Principles of the Law, Data Privacy § 7:

> *1.* In 1973, the U.S. Department of Health, Education, and Welfare (HEW), in its influential report on the harms caused by computer databases, set forth a series of Fair Information Practices, one of which provides that "[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent." U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Commission on Automated Personal Data Systems 41-42 (1973).
>
> *2.* In the United States, a number of federal statutes restrict secondary use. Among the key statutory provisions are the Privacy Act, 5 U.S.C. § 552a(e)(3)(B); Fair Credit Reporting Act, 15 U.S.C. § 1681b; Gramm–Leach–Bliley Act, 15 U.S.C. § 6802(c); Video Privacy Protection Act, 18 U.S.C. § 2710(e); Driver's Privacy Protection Act, 18 U.S.C. § 2722(a); and Cable Communications Policy Act, 47 U.S.C. § 551(e).

Principles of the Law, Data Privacy § 7, Reporters' Notes *1* and *2* (AM. L. INST. 2020).

These materials are analyzed extensively in those Reporters' Notes, which should be consulted for additional details.

Europe:

It is not easy to find direct equivalents of this Principle. On the one hand, the most obvious parallel would be the right to erasure ("right to be forgotten," cf. CJEU in Case C-131/12 ECLI:EU:C:2014:317 – *Google Spain*) in Article 17 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), whose scope is limited to personal data. According to that right, the data subject has the right to demand from the controller that personal data concerning him or her be deleted without undue delay if certain conditions are met. This also includes cases in which personal data were originally processed unlawfully, the data subject has withdrawn his or her consent (if the processing was based on this consent), or the data subject has objected to the data processing (if he or she has such a right to object). On the other hand, the concept in this Principle (and by Part III as a whole) differs quite substantially from that in the GDPR. Not only is this Principle also—or even primarily—written for non-personal data, this Principle also departs from the approach adopted in the GDPR, according to which the consent to data processing, once given, is the most important factor. That approach—like much else in the GDPR—imposes disproportionate restrictions on the data economy, especially for non-personal data, and it does not effectively protect those who have contributed to the generation of data against those data activities that actually substantially affect them. Indeed, once consent has been given and the formal

requirements imposed by the GDPR on the granting of consent have been met, it would seem that consent has also be given to any self-harm or harm to others. In contrast, these Principles start from the principle of free data processing, and only if a concrete data activity violates fundamental principles of fairness, quite exceptionally, a claim to defend oneself against such data activities is provided.

According to Article 7(1) of the recent Council Mandate on the E-Privacy Regulation (ST_6087_2021_INIT), electronic communications services shall erase electronic communications content or make that data anonymous when it is no longer necessary for the purpose of processing. To a lesser extent, that duty also applies to electronic communications metadata when it is no longer needed for the purpose of providing an electronic communication service (Article 7(2)). Because that is not phrased as an individual right but as a duty of the provider of the electronic communications service, it is unclear under the recent draft whether there is private enforcement for infringements of Article 7 via remedies similar to those in the GDPR (Article 21(1)).

Article 16 of the Digital Content and Services Directive (DCSD) (Directive (EU) 2019/770) gives the consumer a right to require desistance in case of termination of the contract for the supply of digital content or a digital service. According to Article 16(3), the trader shall refrain from using any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader. Article 16(3) also lists four cases in which the interests of the trader outweigh the interests of the consumer: the content (a) has no utility outside the context of the digital content or digital service supplied by the trader; (b) only relates to the consumer's activity when using the digital content or digital service supplied by the trader; (c) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts; or (d) has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content. However, Article 16(3) of the DCSD also has a very different purpose than this Principle because Article 16 of the DCSD does not in any way refer to harm suffered by the consumer. The test in subparagraph (b)(i) of this Principle faintly resembles the compatibility test set out in Article 6(4) of the GDPR. If a controller wishes to process data for a purpose other than that for which the personal data have been collected, the secondary purpose must be compatible with the primary purpose, considering (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data; (d) the possible consequences of the intended further processing for data subjects; and (e) the existence of appropriate safeguards, which may include encryption or pseudonymization.

An obligation to desist from the use of data that is based on considerations of unequal bargaining power rather than data protection has been included in the recent proposal for a Digital Markets Act (DMA) (Regulation (EU) 2022/1925). Core platform services that function as gatekeepers may have a dual role, i.e., provide core platform services to business users while competing with those same business users in providing services or products to end users. This dual role allows gatekeepers to gain an advantage by using data, generated from transactions by their

business users on the core platform, for the purpose of their own services that offer similar services to those of their business users. Thus, Article 6(1) of the DMA obliges gatekeepers to refrain from using any aggregated or non-aggregated data, which may include anonymized and personal data that is not publicly available, to offer similar services to those of their business users (see Recital 43 DMA).

The Data Act proposal (COM(2022) 68 final) sets out obligations to desist from data activities that might harm the interest of a party that has contributed to the generation of data for two different constellations: the first one protects the legitimate interests of the data holder, while the second protects those of the user of the "Internet of Things" (IoT) product. According to Articles 4(4) and 6(2)(e) of the Data Act proposal, users or third-party recipients that have obtained data under Article 4 or 5 (see the Reporters' Notes to Principles 18 and 20) shall not use that data to develop a product that competes with the product from which the data originates, or share the data with another third party for that purpose. The second obligation can be found in the second sentence of Article 4(6) of the Data Act proposal, which provides that a data holder shall not use non-personal data generated by the use of an IoT product or related service to derive insights about the economic situation, assets, and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active. A corresponding provision exists in Article 5(5) of the Data Act proposal.

Principle 22. Correction of Co-Generated Data

Grounds that, subject to Principle 19, may give rise to a party's right to require that the controller correct errors in co-generated data, including incompleteness of the data, should include situations in which control or processing of the incorrect data may cause more than insignificant harm, including non-economic harm, to that party's or another party's legitimate interests, and the costs of correction are not disproportionate to the harm that might otherwise result.

Comment:

a. Right to require correction. Poor data quality is a major problem for the data economy. While normally the controller itself should have the greatest interest in improving the quality of data controlled, there may be situations in which the controller happens not to care, but another party who has co-generated the data does care.

Illustration:

107. Business T produces tires that are supplied to car manufacturer C and installed on cars. Data collected by the car sensors is supposed to reveal, inter alia, how well T's tires adapt to different weather conditions and road surfaces and how quickly the treads

wear off. Due to an error in programming the software in cars manufactured by C, the data suggests that tires produced by T fail to adapt well to wet surfaces. This data is added to a pool of car data, to which other car manufacturers also have access. While C may not be sufficiently interested in correcting the data (e.g., because C itself is already aware of the error and does not mind if its competitors draw inaccurate conclusions), T has a strong interest in the error in the data being corrected.

It is in such circumstances that, according to this Principle, a right should be afforded to the other party to request correction of the data. The factors that should be taken into account are listed in Principle 19(2). Among the legitimate interests the controller may raise in denying the request are the costs and efforts of correction and the potential effectiveness of such correction in preventing loss to the party seeking the correction. Given the general interest to improve the quality of data in the data economy, rights to require correction will very often be afforded, except when such a request is vexatious or totally unreasonable or otherwise abusive, or disproportionately costly. If appropriate, in particular when the party requesting correction has contributed to the incorrectness or incompleteness of the data, this party may have to bear a proportionate part of the costs under Principle 19(3).

REPORTERS' NOTES

United States:

Correction of data that is co-generated (within the meaning of that term in these Principles) is addressed in § 8 of the Principles of the Law, Data Privacy, which provides that "[a] data controller shall provide a data subject with a reasonable process to challenge the accuracy of the data subject's personal data" and that "[w]hen a data subject provides a reasonable basis in proof to demonstrate that the data subject's personal data is incorrect, the data controller shall correct the data by amending or deleting it, or by other means." Principles of the Law, Data Privacy § 8(d)(1) and (2) (AM. L. INST. 2020). As stated in that Section, "One of the most universally accepted Fair Information Practice Principles (FIPPs) concerns rights of access and correction." Id., Reporters' Note *1*. Federal law, both statutory and by administrative regulations, establishes some rights of correction. For example, regulations under the Health Insurance Portability and Accountability Act (HIPAA) provide that an individual has a right "to have a covered entity amend protected health information," 45 C.F.R. § 164.526(a)(1). Also, the federal Privacy Act (which addresses certain governmental records) provides that "[e]ach agency . . . shall (1) [permit an] individual . . . to review the record" and "(2) request amendment of a record." 5 U.S.C. § 552a(d)(2).

At the state level, the California Consumer Privacy Act does not provide for a right of correction, nor would several other data privacy bills introduced in U.S. state legislatures. See, e.g.,

proposed Maryland Online Consumer Protection Act Maryland (S.B. 613, 439th Gen. Assemb., Reg. Sess. (Md. 2019), introduced February 4, 2019), proposed Massachusetts Consumer Data Privacy Act (S.B. 120, 191st Gen. Court, Reg. Sess. (Mass. 2019), introduced January 11, 2019), proposed Hawaii legislation "Relating to Privacy" (S.B. 418, 30th Leg., Reg. Sess. (Haw. 2019) introduced January 18, 2019), and proposed North Dakota legislation relating to protection against the disclosure of personal information (H.B. 1485, 66th Leg., Assemb., Reg. Sess. (N.D. 2019) introduced January 14, 2019). In contrast, proposed New York legislation provides that "on request from a consumer, the controller, without undue delay, shall correct inaccurate personal data concerning the consumer." See proposed New York Privacy Act § 1103.2 (S. 5462, 2019-2020 Leg., Reg. Sess. (N.Y. 2019), introduced May 9, 2019).

Europe:

A similar right can be found, in relation to personal data, in Article 16 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). That provision entitles the data subject to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning the data subject. The data subject also has the right to have incomplete personal data completed, including by means of a supplementary declaration. That provision applies, in particular, if the storage of such data violates the GDPR or Union or Member State law to which the controller is subject (see Recital 65 GDPR). Thus, it aims to ensure one of the guiding principles of the GDPR, namely data accuracy, which means that data must be accurate and, when necessary, kept up to date, and that all reasonable steps must be taken to ensure that personal data that are inaccurate are erased or rectified without undue delay (Article 5(1)(d) GDPR). In assessing whether inaccurate data must be erased or rectified, the purpose for which the data are processed must be taken into account.

Principle 23. Economic Share in Profits Derived from Co-Generated Data

(1) A party is normally not entitled to an economic share in profits derived by another party from the use of co-generated data unless there is a contractual or statutory basis for such a claim or it is part of an individual arrangement under Principle 19(3).

(2) Notwithstanding paragraph (1), in exceptional cases, a party may be entitled to an economic share in profits derived by a controller of co-generated data from use of the data when:

(a) that party's contribution to the generation of the data

(i) was sufficiently unique that it cannot, from an economic point of view, be substituted by contributions of other parties, or

(ii) caused that party significant effort or expense;

(b) profits derived by the controller are exceptionally high; and

(c) the party seeking an economic share was, when its contribution to the generation of the data was made, not in a position to bargain effectively for remuneration.

Comment:

a. General observations. Whether producers of data should be entitled to an economic share in the value created with the help of the data is a very controversial topic. Due to the dynamic nature of data, the multitude of parties that contribute to the generation of data, and the nature of data as a non-rivalrous resource, it would be neither possible nor desirable to recognize a general data right of that kind. Rather, when the situation is such as to allow a controller of data to use the data rightfully and to benefit from the use, that controller should be free to do so without having to share the benefits with anyone else. To avoid injustice, however, paragraph (2) of this Principle provides an exception under which a party can, in exceptional circumstances, obtain a share of the profits.

The main reasons for not affording a general rule requiring remuneration for the use of co-generated data are of a practical nature. Introducing claims for remuneration across the board, or at least on a broad scale, would require encompassing and ubiquitous measurement of data flows and would make life for businesses and consumers alike much more complicated. It would be extremely difficult to find a general remuneration scheme that is equitable, and, given that businesses are likely to pass the additional costs on to their customers in the form of higher prices for goods and services, it would result in customers who generate less data subsidizing customers who generate more data, which is questionable from a policy point of view. In light of the fact that measurement of data flows, calculation of reimbursements, and payment management would mean additional costs, a general rule requiring remuneration might well mean less prosperity for everyone. Further considerations include the creation of inappropriate incentives for vulnerable individuals, such as minors or individuals in economic distress, to generate and disclose as much data as possible.

b. Monetary remuneration or compensation on other grounds. This Principle addresses only the possibility of a right to an economic share that is based exclusively on the fact that data has been co-generated by the party exercising the right. It does not address rights to an economic share based on other grounds, such as a contractual agreement. Likewise, when data is used wrongfully, there may be remedies on the part of any party whose rights have been harmed or infringed, and such remedies may include the payment of money.

Illustration:

108. Driver D of a connected car produced by P contributes to the generation of large amounts of data, including data collected by the car's sensors that are not related to the functioning of the car or any services provided to D. P then uses that data for creating very valuable smart services. If, under applicable consumer legislation, the clause in the contract between D and P about the use of D's car for this purpose is void, this may give rise to a claim in unjust enrichment on the part of D.

Also, remuneration may be part of arrangements within the meaning of Principle 19(3). However, independent and separate remuneration is normally not due.

c. Exceptional nature of the right. It is only under very exceptional circumstances that a party may have an independent claim for an economic share in profits derived with the help of co-generated data. This is the case under circumstances similar to those giving rise to intellectual property rights and similar rights, i.e., there must either be a particularly unique contribution or an extraordinary investment. However, the threshold here is much higher than for intellectual property rights, and there must be additional circumstances that make it unfair and inconsistent with doctrines such as unjust enrichment for the party making the profit not to share it with those who have contributed. Additional circumstances of this sort might arise from the exceptional amount of profits derived by the controller, combined with the fact that, when the contribution to the generation of the data was made, the contributing party was, for reasons attributable (also) to the controller, not effectively in a position to bargain for remuneration.

Illustration:

109. Cancer patient P has an extremely rare genetic pattern, inherited from indigenous ancestors, which allows him to overcome the cancer. Without telling P, hospital H uses P's genetic data for developing a new method of cancer treatment, which H then sells worldwide, deriving profits of several billion U.S. dollars. This is a situation in which the data contributed by P is particularly unique, profits derived are exceptionally high, and in the situation (when P was being treated as a patient, worrying about cancer, and P had no idea about the value of the data), P was unable to effectively enter into negotiations with H concerning remuneration.

However, if only the aggregate contributions of many parties contributing in the same way or in similar ways to the generation of data have the effect described in this Principle, those contributors would not generally have a right to share in the profits.

Illustration:

110. Driver D of a connected car produced by M contributes to the generation of large amounts of data, which M then uses, together with the data generated by thousands of other drivers, for creating very valuable smart services, deriving profits of billions of U.S. dollars. Even if D's mobility profile may be unique, it can, from an economic point of view, at any time be substituted with some other driver's data. Also, generating the data does not require extraordinary effort or expense on the part of D. D does not have a right to claim a share in M's profits.

REPORTERS' NOTES

United States:

For a recent discussion of the issues raised here, see, e.g., Jorge L. Contreras, *The False Promise of Health Data Ownership*, 94 N.Y.U. L. REV. 624 (2019).

Comment *c* and Illustration 109 are inspired by the story of Henrietta Lacks. See REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS (2010). It has been reported that "There are 17,000 U.S. patents that involve HeLa cells." *Can the "Immortal Cells" of Henrietta Lacks Sue for their Own Rights?*, WASH. POST (June 25, 2018), https://www.washingtonpost.com/news/retropolis/wp/2018/06/25/can-the-immortal-cells-of-henrietta-lacks-sue-for-their-own-rights/, quoting Christina J. Bostick, an attorney who is representing several descendants of Ms. Lacks. See also *The Legacy of Henrietta Lacks*, Johns Hopkins Medicine, https://www.hopkinsmedicine.org/henriettalacks/frequently-asked-questions.html (last visited May 18, 2020), noting that "Johns Hopkins has never sold or profited from the discovery or distribution of HeLa cells and does not own the rights to the HeLa cell line."

A well-known case rejecting an economic share of profits, albeit in response to a claim raising somewhat different legal theories, is Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990), cert. denied, 499 U.S. 936 (1991). But see Greenberg v. Miami Children's Hosp. Rsch. Inst., Inc., 264 F. Supp. 2d 1064 (S.D. Fla. 2003) (finding that plaintiffs sufficiently pleaded the requisite elements of an unjust enrichment claim).

Europe:

A major aspect of the discussion around "data ownership" was the allocation of a fair share of the economic value of data to parties who have contributed to the generation of data. Allocating the income is normally a function of intellectual property rights (see Article 18 Copyright Directive, Directive (EU) 2019/790). Suggestions were made, e.g., to have collective societies

manage individuals' economic rights in their personal data (cf. Karl-Heinz Fezer, Repräsentatives Dateneigentum – Ein zivilgesellschaftliches Bürgerrecht, 2018, p. 84 f.). There has been strong resistance against such a model, primarily for the reasons stated in the Comments to this Principle (e.g., Josef Drexl, Data Access and Control in the Era of Connected Devices, 2018, p. 144, Opinion of the German Data Ethics Commission, 2019, p. 104 f.). Thus, there is currently no such right to share in profits in Europe, and it seems unlikely that it will be introduced in the near future.

However, the factors listed as relevant for granting such a right in very exceptional circumstances—uniqueness, investment, profit, and lack of negotiability—are known from European intellectual property law. Thus, the protection of copyright and similar rights applies only if the work is the author's own intellectual creation (cf. Art. 1(3) Software Directive, Directive 2009/24/EC; Art. 3(1) Database Directive, Directive 96/9/EC), which requires that the work be sufficiently original or unique (cf. CJEU Case C-5/08 ECLI:EU:C:2009:465 para. 37 – *Infopaq*). The protection of investment made is provided by rights such as the *sui generis* right of the Database Directive (see Article 7 Directive 2009/24/EC). Finally, under the exhaustion principle, profit and lack of negotiability are the main arguments for protection until the first sale of a copy. The first sale of a copy of a computer program by the rightholder exhausts the distribution right in that copy (cf. Article 4(2) Information Society Services Directive, Directive 2001/29/EC; Article 4(2) Software Directive) because the rightholder already had the opportunity to obtain a fair remuneration at the first sale of the copy (cf. CJEU Case C-128/11 ECLI:EU:C:2012:407, para. 63 – *UsedSoft*). However, there are two important exceptions to this principle: the first is that the author still has the right to control the subletting of the program or a copy thereof (Article 4(2) Software Directive). The second exception is enshrined in Article 20 of the Copyright Directive (Directive (EU) 2019/790), which applies when the remuneration originally agreed by the author turns out to be disproportionately low compared to any subsequent relevant income from the exploitation of the works or performances. In such cases, the author—in the absence of an applicable collective bargaining agreement—is entitled to demand additional reasonable and fair remuneration from the party with whom the author has concluded a contract for the exploitation of his or her rights.

CHAPTER C
DATA RIGHTS FOR THE PUBLIC INTEREST

Principle 24. Justification for Data Rights and Obligations

(1) The law should afford data rights for reasons of the public interest, independent of the share that the party to whom the rights are afforded had in the generation of the data, only if the encroachment on the controller's or any third party's legitimate interests is necessary, suitable, and proportionate to the public interest pursued.

(2) Paragraph (1) is not intended to address intergovernmental relations.

(3) The proportionality test referred to in paragraph (1) should apply also for determining the specifications or restrictions of data rights, such as concerning data formats, timing, data security, further support required for exercise of the right to be fully effective, and remuneration to be paid.

(4) If the law does not afford a data right but imposes a functionally equivalent data sharing obligation, the Principles under this Chapter apply with appropriate adjustments.

Comment:

a. Data rights motivated by the public interest. This Principle refers to data rights that are not based on the share that a party had in the generation of the data. A data right, in particular a data access right, is conferred on a person that has no specific relationship with the way the data was generated (i.e., the person is not the subject of the information and has not produced or assembled the data). The type of data right addressed in Principles 24 to 27 is, therefore, of a different nature from the rights addressed in Chapter B. While the rights provided in Chapter B are clearly of a private law nature and follow something like a "property logic," the rights addressed in Chapter C are more of a public law nature. In practice, they are almost exclusively about data sharing, i.e., data rights within the meaning of Principle 16(1)(a), but could theoretically also include other types of data rights.

Illustration:

111. Farmer F has purchased a connected tractor, manufactured by M. After an engine breakdown, F wants to have his tractor repaired at independent repair shop R. To repair the tractor, R needs access both to data generated by the tractor while it was used by F and to other data held by M to adjust the engine correctly. F himself would definitely

have a right under Chapter B to access the former data as it has been co-generated by F (but see Principle 20(1)(a)), and arguably also a right to access the latter data, taking into account that this is further support required to make access to the co-generated data fully effective (but see Principle 19(3)). However, in order for independent repair shops like R to fulfill their function properly, it is not sufficient to give just F an individual right to access data relating to F's tractor—rather, R needs more general access to such data held by M, e.g., in order to train and prepare for such types of repair. If the law affords such access to R, this access is governed by the Principles under Chapter C, because R did not share in the generation of the data.

Data rights within the meaning of Chapter C frequently overlap with competition law, which primarily serves the purpose of ensuring undistorted competition for the benefit of everyone, and may result in particular private parties having a data right against, for example, another party with a dominant market position. There may be many other public-interest considerations that can lead a legislator to afford data rights of the sort addressed in this Chapter, such as enhancement of research and development, more efficient use of research money, and reduction of unnecessary testing by imposing an obligation to share research data and results. There is also a growing debate about the extent to which controllers of data can be forced to share certain data with actors in the public-services sector, such as in the health, mobility, and energy sectors.

Given the variety of public interests potentially at stake, these Principles do not give specific guidance as to the circumstances under which such data sharing obligations may be imposed. Rather, these Principles restrict themselves to guidance concerning some core aspects that need to be taken into account when a decision to impose such data sharing obligations or similar obligations has been made. The notion of "public interest" should be understood very broadly to include rules that vindicate or establish private rights for reasons of the public interest. Antitrust and competition laws are a good example of this phenomenon.

b. Justification for encroachment. The main purpose of this Principle is to clarify that the affording of such data rights and the imposition of such data obligations amounts to an interference with the interests of private parties and is thus in need of justification. In contrast, data rights and data obligations under Chapter B may be seen simply as an attempt by the law to strike the right balance between competing private interests. In deciding whether to afford data rights under this Principle, the public interest needs to be carefully weighed against the interests of the controller,

which may even be protected by fundamental rights. Data rights for the public interest may not only encroach on the rights of the controller but also affect the protected interests of other parties, such as data subjects (in the case of personal data) or the holders of intellectual property rights (when the data is protected by intellectual property rights). Their interests must also be duly taken into account when granting data rights for the public interest. In light of all these conflicting interests, the data right must be necessary and suitable to achieve the objective, and must be a proportionate means.

If a data right in the public interest is afforded to a party that contributed to the generation of the data, the threshold is lowered. For example, if simply creating a statutory data access right for the public interest, and a corresponding encroachment on the rights of the controller, would normally not pass the proportionality test, the legislator may resort to a portability right (afforded to a party that had contributed to the generation of the data) as a vehicle. The fact that a party has contributed to the generation of data is already in itself part of a separate justification for affording a data right and encroaching the controller's interests (see the Comments to Principles 18 and 19). However, the Principles of Chapter C can still be of relevance, for example, concerning access conditions that are fair, reasonable, and nondiscriminatory.

c. Limited need for justification for open data in the public sector. The considerations in paragraph (1) relate primarily to governmental decisions to afford data rights against controllers in the private sector. In light of the complexities of intergovernmental relationships, paragraph (2) provides that paragraph (1) does not address data rights as against a controller in the public sector. A governmental decision to afford data rights against a data controller in the public sector raises fewer issues than a decision to afford such rights against a data controller in the private sector because, in the latter case, there is interference with economic rights of the controller while there may not be such interference with economic rights in the case of public entities. It is often a purely political consideration whether making public-sector data freely available is a reasonable way of helping the economy and spending taxpayers' money. Of course, if the controller is a public entity and the data it controls are personal data or other data affecting legitimate interests of third parties (such as those referred to in Principle 28), these third-party interests still need to be fully protected.

d. Application of the proportionality test to modalities. In line with Principle 19(3), paragraph (3) of this Principle clarifies that the proportionality test applies not only to whether or not a right should be afforded and/or an obligation imposed, but also to any specifications or restrictions, such as concerning data formats, mode of access, timing, data security, further support

required for exercise of the right to be fully effective, and remuneration to be paid. In particular, remuneration of the controller or other affected parties may be needed to make the imposition of an obligation a proportionate measure.

Illustration:

112. Assume that the law grants independent repair shops, such as R in Illustration no. 111, a data access right against the controllers of vehicle data such as M. In granting the right, the law should make adequate provision for M's legitimate interests, such as concerning protection of trade secrets, as well as the legitimate interests of third parties, such as the trade secrets of any suppliers of components or, if the aggregated vehicle data allows inferences with regard to other customers, the privacy and secrecy concerns of other customers. This may mean that R should not be afforded a right to access all tractor-related data on M's servers, but only data that is necessary for R to fulfill its functions, and data may need to be preprocessed so as not to allow inferences on other customers or disclosure of trade secrets. Given also that R is acting for commercial purposes, it may be appropriate for the law to allow M to charge a reasonable fee.

e. Functionally equivalent data sharing obligations. Data rights afforded without regard to a party's share in the generation of the data are mostly data rights afforded for the public interest. Nothing in this Principle excludes the possibility that such data rights are afforded also with a view to the protection or promotion of private interests, but it is much more common that private parties are just the incidental beneficiaries of data rights, while the data rights were primarily afforded for the public interest. This becomes all the more apparent in cases in which the law primarily imposes an obligation on the controller of data to share data with a particular class of parties, should those parties be interested in the data, or even with the general public. Paragraph (4) therefore states that the Principles under this Chapter apply with appropriate adjustments when the law does not focus on the right, but instead on a functionally equivalent obligation.

Illustration:

113. In order to aid independent repair shops like R in Illustration no. 111 in fulfilling their function, the law may either give repair shops like R an individual access right against data controllers like M, or impose an obligation on M to make tractor data available on some kind of platform, usually for a specific class of parties (i.e., independent

repair shops like R), with failure to comply with this obligation primarily triggering sanctions under administrative law.

REPORTERS' NOTES

United States:

Data rights for the public interest have not developed extensively in the United States. One exception to this generalization is legislation mandating some form of public access to governmental data. On the federal level, see the Open, Public, Electronic, and Necessary Government Data Act, Pub. L. 115–435, Title II, Jan. 14, 2019, 132 Stat. 5534. On the local level, see, e.g., New York City Local Law 11 of 2012 and subsequent implementing legislation (codified as amended at N.Y.C. ADMIN. CODE § 23.501-23.503 (2018)).

Legislation mandating data rights with respect to private data has been less common. One exception relates to automobile repair data. See MASS. GEN. LAWS ch. 93K, § 2 (providing for access by owners of motor vehicles and by independent repair facilities to motor vehicle manufacturer diagnostic and repair information and diagnostic repair tools otherwise made available to dealers). By ballot initiative in 2020, Massachusetts voters approved Question 1, which augments Chapter 93K. The summary of the initiative provided in part that:

> This proposed law would require that motor vehicle owners and independent repair facilities be provided with expanded access to mechanical data related to vehicle maintenance and repair.
>
> Starting with model year 2022, the proposed law would require manufacturers of motor vehicles sold in Massachusetts to equip any such vehicles that use telematics systems –- systems that collect and wirelessly transmit mechanical data to a remote server –- with a standardized open access data platform. Owners of motor vehicles with telematics systems would get access to mechanical data through a mobile device application. With vehicle owner authorization, independent repair facilities (those not affiliated with a manufacturer) and independent dealerships would be able to retrieve mechanical data from, and send commands to, the vehicle for repair, maintenance, and diagnostic testing.
>
> Under the proposed law, manufacturers would not be allowed to require authorization before owners or repair facilities could access mechanical data stored in a motor vehicle's onboard diagnostic system, except through an authorization process standardized across all makes and models and administered by an entity unaffiliated with the manufacturer.
>
> The proposed law would require the Attorney General to prepare a notice for prospective motor vehicle owners and lessees explaining telematics systems and the proposed law's requirements concerning access to the vehicle's mechanical data. Under the proposed law, dealers would have to provide prospective owners with, and prospective owners would have to acknowledge receipt of, the notice before

> buying or leasing a vehicle. Failure to comply with these notice requirements would subject motor vehicle dealers to sanctions by the applicable licensing authority.

Mass. Sec'y of State, 2020 Voter Guide, Ballot Question 1.

That law is the subject of a lawsuit by the Alliance for Automotive Innovation, seeking to enjoin enforcement on preemption and takings grounds. See Complaint, All. for Auto. Innovation v. Healey, No.1:20-cv-12090 (D. Mass. Nov. 20, 2020). See also Matthew Gault, *Newly Passed Right-to-Repair Law Will Fundamentally Change Tesla Repair*, VICE (Nov. 10, 2020), https://www.vice.com/en/article/93wy8v/newly-passed-right-to-repair-law-will-fundamentally-change-tesla-repair; Corynne McSherry, *Who Will Own the Internet of Things? (Hint: Not the Users)*, ELEC. FRONTIER FOUND. (Jan. 20, 2015), https://www.eff.org/deeplinks/2015/01/who-will-own-internet-things-hint-not-users.

Europe:

The European Union has already introduced several sector-specific instruments that grant access rights to parties who have not contributed to the generation of the data. Because these access rights need to be not only justified by a public interest but also necessary and proportionate, they are limited to certain situations in which the European legislator deems the public interest to outweigh the interest of the controller, and only cover data that is necessary to achieve the objective pursued. Political consensus may develop for the adoption of additional data rights for the public interest.

One of the most prominent examples for an access right against the controller by a party that has not contributed to the generation of the data is in the Type Approval Regulation (Regulation (EU) 2018/858). Article 61 of that Regulation obligates car manufactures to grant independent maintenance and repair service providers access to the technical information necessary to perform their services in a non-discriminatory way for fees that are reasonable and proportionate. The rationale of that access right is that, due to the complexity of today's vehicles, independent repair service providers, as well as spare part producers, can only offer their services and products if they have access to the necessary technical information. Because the access right of the independent service providers interferes with the contractual freedom of car manufacturers as well as their freedom to conduct business (Article 16 Charter of Fundamental Rights), it needs to be justified by a legitimate public interest. In this case, the public interest is to prevent a market failure on the aftermarket, which would lead to higher prices, lower quality of services, less innovation, and less choice for consumers. The market failure tendencies in the aftermarket in the automotive sector have been a longstanding issue. Car manufactures try to forestall effective competition by denying access to brand-specific technical information in order to promote authorized dealers and repairers, which has proven to be very profitable for the manufacturers. However, by allowing the manufacturers to charge a reasonable fee for data access, the Type Approval Regulation also takes into account the legitimate interest of manufacturers to receive a fair return on their investment. The Type Approval Regulation serves as an example for an instrument that primarily aims at promoting a public interest (functioning aftermarket), although

the access right is afforded only to a handful of the private parties (independent repair and maintenance service providers), who thus also benefit from the access right.

The public interest that justifies an access right may be something other than a functioning market, as demonstrated by the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation (Regulation (EC) No 1907/2006). Article 27 of that Regulation gives a manufacturer seeking to register a chemical substance (registrant) a right against manufacturers who have already registered such a substance to access their testing data for tests of the substance on animals. The rationale is to avoid unnecessary duplication of tests that have a significant impact on the environment and cause unnecessary harm to animals (Recital 40). The initial registrants shall receive a fair, transparent, and non-discriminatory compensation for making the testing data available to the potential registrant.

While data access and sharing rights afforded to the user of an "Internet of Things" (IoT) product under the Data Act proposal (COM(2022) 68 final) are primarily rights in co-generated data within the meaning of Principle 18 (see the Reporters' Notes thereto), they also have characteristics of data rights in the public interest. Recital 25 clarifies that the access (Article 4) and sharing (Article 5) rights are not only afforded to strengthen the position of the user but also to allow smaller innovative businesses to enter the market and offer data-based solutions for IoT products in a competitive manner.

Data access rights may also follow from general doctrines of competition law. The basic line of reasoning is that the aggregation of large datasets in the hands of a single market player may constitute an abuse of a dominant position, and would thus justify an interference with the rights of the data holder for the benefit of the general public. In Europe, there is an extensive debate as to whether this result can be achieved with the existing doctrines of competition law (for an overview, see Wolfgang Kerber, Updating Competition Policy for the Digital Economy?, 2019). The most promising candidate is the so called "essential facilities doctrine" (EFD), as it is designed to address cases in which a dominant market player refuses without objective justification to grant access to a resource that is essential for a downstream market and thereby eliminates effective competition. As the name suggests, the test was originally developed for cases of denied access to physical facilities, such as ports. Later, the notion was expanded to cases in which access to information was denied based on intellectual property rights. With data being digitized information, the EFD seems to be very fitting for cases of denied access to data. However, a closer look reveals that the requirements that have been developed by the Court of Justice of the European Union (CJEU) cannot easily be applied to situations of denied access (Heike Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welker, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018, p. 131 ff.; Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, Competition policy for the digital era, 2019, p. 98 ff.; Furmann et al., Unlocking digital competition, Report for the Digital Competition Expert Panel, 2019, pp. 55 ff). Thus, some authors argue for a "fresh" balancing of interests without regard to the established confines of the EFD (Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, Competition policy for the digital era, 2019, p. 98 ff). However, the main constraints of competition law are its intervention threshold and intervention timeframe. It is even in highly concentrated markets, such as the markets for cloud service providers or business-to-consumer (B2C) market platforms, very

difficult to prove the existence of a dominant market position under Article 102 of the Treaty on the Functioning of the European Union (TFEU). Furthermore, competition law enforcement is time consuming, and the relevant market might be fundamentally transformed or potential innovative business models might disappear before an ad-hoc competition case decision is validly taken and implemented (see Dirk Staudenmayer, Towards a European Private Law of the Digital Economy?, in André Janssen and Hans Schulte-Nölke (eds.), Researches in European Private Law and Beyond, 2020, p. 65, 84 ff). This is why it has been argued that ex post competition law enforcement should be complemented with ex ante regulation to prevent market tipping, ensure market contestability, and stimulate innovation (see Bertin Martens et al, JRC Digital Economy Working Paper 2020-05, Business-to-Business data sharing: An economic and legal analysis, 2020, p. 35 ff).

Public interests play an even more significant role in business-to-government (B2G) data sharing relationships. Access to data is crucial when dealing with the growing number of societal challenges such as climate change, natural disasters, urban planning, or pandemics. For these reasons, the proposal for a Data Act (COM(2022) 68 final) addresses B2G data sharing in a separate Chapter. According to Article 14 of that proposal, public bodies shall have the right to request access to privately held data if certain public interests are at stake. Such "exceptional needs," which justify the encroachment of the data holder's interests, shall be deemed to exist if the data requested is necessary to respond to a public emergency (Article 15(a)); or if the data requested is limited in time and scope and necessary to prevent a public emergency or to assist in the recovery from a public emergency (Article 15(b)). Furthermore, public sector bodies or Union institutions, agencies, or bodies may be prevented from fulfilling a specific task in the public interest due to a lack of available data (Article 15(c)). The last case is only considered an exceptional need if the public sector body has been unable to obtain such data by alternative means, such as by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data (Article 15(c)(1)); or if obtaining the data in line with the procedure laid down in Articles 14 ff of the Data Act proposal would substantively reduce the administrative burden for data holders or other enterprises (Article 15(c)(2)). In line with Principle 26(2), the public interest and the proportionality test not only determine whether a public body may access privately held data based on Article 14 of the Data Act proposal, but also under what conditions. If the requested data is necessary to prevent a public emergency or to assist the recovery from a public emergency, the data must generally be made available free of charge (Article 20(1) Data Act proposal). This part of the Data Act proposal is inspired by Principles 24 through 27, as well as the recommendations of the report of the Expert Group on B2G Data Sharing (COM(2020) 66 final, p. 12). In its final report, the Expert Group recommended the creation of an EU regulatory framework providing a minimum level of harmonization for B2G data-sharing processes (High-Level Expert Group on Business-to-Government Data Sharing, Towards a European strategy on business-to-government data sharing for the public interest – final report, 2020, p. 41 ff.). The Expert Group's proposed data-sharing requirements have some significant overlaps with the approach chosen in Principles 24 through 27. One of the main features the two approaches have in common is their flexibility. The framework of the Expert Group should also apply without prejudice to the applicable legal

frameworks, e.g., for personal and non-personal data, and should further allow Member States to choose rules compatible with their legislation or applicable to the specific sector.

The obligation to share data in the public sector is also discussed under "open government data" or "public-sector information." The sharing of data between public bodies and private enterprises (open government data) is regulated in the Open Data Directive (Directive (EU) 2019/1024) for EU institutions. Regarding research data, the Organisation for Economic Co-operation and Development (OECD) stated in 2006 that openness means "access on equal terms for the international research community at the lowest possible cost, preferably at no more than the marginal cost of dissemination" (see OECD, Recommendation of the Council concerning Access to Research Data from Public Funding, 2006, III.B.). Most definitions of "open data" beyond research data include non-discriminatory access, costs of access, and—in some cases—redistribution (see OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 41 f.). A prominent example of a definition of "open data" can be found in the International Open Data Charter, which defines "open data" as "digital data that is made available with the technical and legal characteristics necessary for it to be freely used, re-used and redistributed by anyone, anytime, anywhere" (International Open Data Charter, https://opendatacharter.net/principles/). See further the Reporters' Notes to Principle 25.

Justification plays a completely different role with regard to open government data. Rather than looking for a justification for why open government data should be shared, governments need to justify why data should not be shared (see Principle 1 International Open Data Charter, https://opendatacharter.net/principles/). This is often simply expressed with the term "open by default," which is a general recognized principle of open government data (see Principles 1 and 3 G8 Open Data Charter signed at the G8 Summit on 18 June 2013; Recital 16 of Directive (EU) 2019/1024). Typical exemptions to that rule are security or data protection concerns. See further the Reporters' Notes to Principle 26.

Principle 25. Granting of Data Access by the Controller

(1) If the law affords a data access right within the meaning of Principle 24, the law should provide that the controller must provide access under conditions that are fair, reasonable, and nondiscriminatory within the class of parties that have been afforded the right.

(2) Consistent with Principle 24(3), a data access right should be afforded only with appropriate restrictions such as disclosure to a trusted third party, disaggregation, anonymization, or blurring of data, to the extent that affording the right without such restrictions would be incompatible with the rights of others, or with public interests.

(3) The controller must comply with the duties under Principle 32 for the protection of third parties, and restrictions under paragraph (2) must in any case enable the controller to do so.

Comment:

a. Relationship of Principles 24 and 25. This Principle contains recommendations for two important issues that should be addressed in a law of the sort described in Principle 24. Both issues concern some of the essential duties a controller must fulfill when granting access to a party seeking access to data on the basis of such a law. These recommendations may also be used by courts as a source of supplementary principles for applying legislation that is silent as to these points.

b. Access under fair, reasonable, and nondiscriminatory conditions. Under paragraph (1), the law should provide that the controller must provide data access under conditions that are fair, reasonable, and nondiscriminatory within the class of parties that have been afforded the data access right. As noted above, this recommendation may also be used to supplement legislation that is silent on this point, or when the law leaves the details to negotiations between the controller and the recipient.

Illustration:

114. If M in Illustration no. 112 grants access to vehicle data to R and the law does not state how the remuneration to be paid by R is to be calculated, M must charge R fees that are fair and reasonable, and must not charge R more than M charges other independent repair shops in a comparable situation.

c. Protection of others. Consistent with Principle 20(2), paragraph (2) of this Principle provides that a data access right should be afforded only with appropriate restrictions such as disclosure to a trusted third party, disaggregation, anonymization, or blurring of data, to the extent that affording the right without such restrictions would be incompatible with the rights of others, or with the public interest. The public interest in encouraging the sharing of data for the benefit of innovation and growth may in a given situation be in conflict with the legitimate interests of the controller itself or of third parties. Those legitimate interests may follow from a variety of rights and considerations, ranging from privacy to trade secrets protection to other secrecy concerns. Some of these interests may equally amount to a public interest. While these Principles do not take a stand as to whether the principle of "open by default" or "privacy by default" should generally prevail, paragraph (2) of this Principle stresses the general necessity to tailor the modalities of any data access right to the legitimate interests of others (i.e., the controller or any third party) such as by involving a data trustee or escrowee within the meaning of Principles 13 and 14.

d. Compliance with duties under Principle 32. In a similar vein and consistent with Principle 20(3), paragraph (3) of this Principle provides that the controller, when granting access to data to third parties pursuant to a data right for the public interest, must comply with the general duties of a supplier under Principle 32. This means that, even when access is not granted under a contract, the controller must make sure that all restrictions that the controller itself must observe in the context of data activities with regard to the data in question are imposed on the recipient. This may be achieved by legal, institutional, or technical means.

Illustration:

115. If M in Illustration no. 112 grants access to vehicle data to R, M should have to make sure it takes appropriate steps for the protection of, for example, trade secrets of its suppliers or privacy concerns of other users of tractors. At least, M should have to impose the same restrictions on R by way of a contract, and R should have to accept this. However, this may not be sufficient. Rather, under Principle 32, M may need to take further steps, including technical measures, such as allowing access to and use of the data only within a secure processing environment provided by M.

REPORTERS' NOTES

United States:

The Open, Public, Electronic, and Necessary Government Data Act requires that open Government data assets made available to the public pursuant to the Act must not be "encumbered by restrictions, other than intellectual property rights . . . that would impede the use or reuse of such asset." Open, Public, Electronic, and Necessary Government Data Act, Pub. L. 115–435, Title II, Jan. 14, 2019, 132 Stat. 5534, § 202(a)(20).

Europe:

In Europe, the introduction of access rights to data, based on fair, reasonable, and non-discriminatory (FRAND) terms, has been discussed both on a policy and academic level for several years (COM(2017) 9 final, p. 13; cf. Benoit Van Asbroeck et al., Building the European Data Economy, Data Ownership – White Paper, 2017). FRAND-based access was originally introduced as a remedy in competition law cases to ensure the supply of a particular product or the access to specific infrastructure. For example, in the Microsoft Case, Microsoft was ordered to disclose interoperability information, which was indispensable for producing programs that are compatible with Windows, on a non-discriminatory basis and under terms that are reasonable in order to remedy distortions of competition (European Commission Case COMP/C.3/37.792, 24. Paras. 1005-1008 – Microsoft, 24 March 2004). FRAND terms also play an important role in the licensing of Standard Essential Patents (SEPs), which may cover standard specifications that are essential

for facilitating innovation and a level playing field in the information and communication technology (ICT) sector. Industry stakeholders who invested in the creation and protection of these standards of course have an interest in receiving a return on this investment by way of licensing. However, exclusive rights conferred by patents may defeat the benefits of having industry-wide standards that are available for public use. To strike a balance between these two competing interests, SEP holders are required to license their SEPs on FRAND terms (Y Ménière, 'Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms: Research Analysis of a Controversial Concept,' 2015). It has been proposed that the findings of the Court of Justice of the European Union (CJEU) in the *Huawei* Case (CJEU Case C-170/13 ECLI:EU:C:2015:477 – *Huawei*), on a negotiation framework for the licensing of SEP on FRAND terms, could be used as inspiration for cases of data access (see Josef Drexl, Designing Competitive Markets for Industrial Data - Between Propertisation and Access, [2017] JIPITEC 257, 285). Thus, it could assist the parties to reach an agreement on the price of access (see Thomas Tombal, Economic dependence and data access, [2020] International Review of Intellectual Property and Competition Law 51:70, 94 f).

Especially in Communications from the European Commission, data access rights based on FRAND terms have repeatedly been discussed as an instrument to address market failures in the data economy (COM(2017) 9 final, p. 13; COM(2020) 66 final, p 13). Some variations of the FRAND principle can be found in connection with sector-specific access rights. For example, the car manufacturer, who according to Article 61 of the Type Approval Regulation (Regulation (EU) 2018/858) must disclose technical information to independent repair service providers (see the Reporters' Notes to Principle 24) "may charge reasonable and proportionate fees for access." Under the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation (Regulation (EC) No 1907/2006), the registrant of a chemical substance must share data regarding tests on vertebrate animals with potential registrants. According to Article 27(3) of that Regulation, "the previous registrant and potential registrant(s) shall make every effort to ensure that the costs of sharing the information are determined in a fair, transparent and non-discriminatory way."

FRAND-based access rights can also be found in the Regulation that established rules for the participation in the European Union's Framework Programme for Research and Innovation (Horizon 2020) (Regulation 1219/2013). Article 48(1) grants participants in the Framework Programme an access right to the results of another participant in the same action if those results are needed by the former to exploit its own results. Subject to an agreement, this access shall be granted under fair and reasonable conditions (Article 48(2)). In Article 2(10) "fair and reasonable conditions" are defined as "conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged."

In the Data Governance Act (Regulation (EU) 2022/868), FRAND is a condition for providing data intermediation services. Article 12(f) of that Act stipulates that the provider of data intermediation services needs to "ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards

prices." Also, the Digital Markets Act (ST 8722/2022 INIT) obligates gatekeepers to provide to any third-party providers of online search engines, upon their request, access to ranking, query, click, and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, on a FRAND basis.

With the proposal for a Data Act, FRAND may become a principle that applies to all data access and sharing (portability) rights scenarios. According to Article 8(1) of the Data Act proposal (COM(2022) 68 final), a data holder that is obliged to make data available to a data recipient under the Data Act or other Union Law or national legislation implementing Union law shall do so under fair, reasonable, and non-discriminatory terms, and in a transparent manner. The data holder is further prohibited from discriminating between comparable categories of data recipients when making the data available (Article 8(3) Data Act proposal) and shall not make data available on an exclusive basis (Article 8(4) Data Act proposal). In addition, any compensation agreed between a data holder and a recipient for making data available shall generally be reasonable (Article 9 Data Act proposal), but when the recipient is a micro-, small-, or medium-sized enterprise (MSME), the compensation agreed shall not exceed the costs directly related to making the data available to the data recipient.

Principle 26. Data Activities by Recipient

(1) If the law affords a data access right within the meaning of Principle 24 to a party, the law should provide that, subject to paragraph (2), the party may utilize the data it receives in any lawful way and for any lawful purpose that is not inconsistent with:

(a) the public interest for which the right was afforded, provided the recipient had notice of that interest;

(b) restrictions for the protection of others imposed under Principle 25(2); or

(c) any agreement between the parties, including an agreement concerning duties and restrictions imposed by the controller on the recipient under Principle 32.

(2) A party to whom a data access right is afforded under Principle 24 may not utilize that data in a way that harms the legitimate interests of the original controller more than is inherent in the purpose for which the right was afforded.

Comment:

a. Freedom of use as the default rule. While Principle 25 sets out basic principles governing the controller's duties, this Principle sets out principles governing the recipient of the data and any data activities this recipient may engage in. When the law imposes a data access right within the meaning of Principle 24 (or an equivalent data sharing obligation) it could provide either that the data may be used exclusively for the purposes for which the right had originally been afforded, or

the law can be more liberal with regard to data use. This Principle recommends that the law should take the latter approach, stating that the recipient may use the data in any lawful way and for any lawful purpose as long as it is consistent with a number of limitations originating either from the law or from the agreement of the parties. This approach is more "open" and may better help foster innovation and growth.

b. Limitations on freedom of use. The data access rights provided for in paragraph (1) must be exercised consistent with three limiting factors. First, the data received may be used only for a purpose that is not inconsistent with the public interest for which the right was afforded. For data use to be inconsistent with the public interest it must actually contravene or undermine that public interest. It is not enough that the type of data use just failed to be contemplated by the legislator when the access right was created.

Illustration:

116. Municipality M is under a statutory obligation to make data from smart road infrastructure freely available. The stated purpose of the statute is to enable businesses to develop smart services for the improvement of the traffic situation. Business B uses the data for developing a service that helps steer smart home equipment, causing air conditioning facilities of premises to stop importing outside air when nearby traffic is dense. This is not a purpose foreseen when the access right was created, and the access right would probably not have been created for that purpose. But, as this innovative use is not explicitly excluded by the relevant statute, and is not inconsistent with the original purpose (and does not harm M, see paragraph (2)), B should be allowed to use the data for this purpose.

However, there are usually also more specific limitations, either imposed directly by the law that affords the access right (see Principle 25(2)) or individually by the controller under an agreement between the controller and the recipient, including an agreement made to ensure that the requirements of Principles 25(3) and 32 are met.

Illustration:

117. Municipality M in Illustration no. 116 makes data that indicates traffic density and the speed at which vehicles are going available to research institute R. In light of the fact that the data includes internet protocol (IP) addresses of connected vehicles, it would

theoretically be possible to create mobility profiles for particular vehicles with the data, which, if combined with other data, could be rather sensitive information, the disclosure of which might harm the legitimate interests of third parties. This is why M makes the data available only under strict conditions, including conditions related to the secure storage of the data and the purposes for which the data may be used. These conditions might already be listed in a law regulating the granting of data access by M, or may be imposed by M on R on a contractual basis in the individual case. R is bound by these conditions.

c. No-harm principle. Situations may arise in which the party benefiting from an access right under Principle 24, or an equivalent data sharing obligation, uses the data in a way that harms the legitimate interests of the original controller. What counts as "harm[ing] the interests of the original controller" should be answered according to general principles, taking into account that inflicting harm on third parties within that controller's sphere of interest may amount to harm inflicted on the controller itself. In many cases, this is almost inevitable, such as when the original controller and the party receiving data are competitors and thus the latter party's competitive gain is mirrored by the original controller's competitive loss. However, when the receiving party uses the data to cause harm to the original controller that goes beyond what is inherent in the purpose for which data sharing was introduced, that violates, at the least, principles of fundamental fairness. It should therefore be prohibited. This is without prejudice to paragraph (1), i.e., when harming the interests of the original controller is already inconsistent with the public interest for which the data access right was afforded, or with additional limitations imposed by the law or by agreement, it may already be prohibited under paragraph (1).

Illustrations:

118. Under an open research data scheme, research institute R1 is obligated to make research data freely available. Research institute R2 uses the data to advance its own research, saving millions in investment, and gains a decisive competitive edge over R1 in a competition for public funds. Use of the data by R2 harms the interests of R1, but this harm is inherent in the purpose for which the obligation to share research data was imposed, so R2 is not acting in violation of paragraph (2) of this Principle.

119. In a situation such as that in Illustration no. 118, research institute R2 uses the research data published by R1 to prove that R1 has forged research results, pretending to have actually run laboratory trials that were really just simulated by a computer. The

detection of research fraud is within the range of purposes of open research data regimes, so R2 is not acting in violation of paragraph (2) of this Principle.

120. In a situation such as that in Illustration no. 118, research institute R2 uses the research data published by R1 for building a "digital twin" of an important unit within R1, trying to predict each of R1's moves and to be quicker in publishing and in forging strategic alliances. A court could find that this harms R1's legitimate interests and is not at all inherent in the purpose for which the law introduced the open research data regime, and therefore that R2 has violated paragraph (2) of this Principle.

The controller, for purposes of paragraph (2) of this Principle, may be a public or private entity. In particular when the controller is a public entity, the range of parties within the controller's sphere of interest may be very broad.

Illustration:

121. In a situation such as the one described in Illustration no. 116 municipality M makes data from smart road infrastructure freely available. Among other things, the data indicates traffic density and the speed at which vehicles are going. Business B uses artificial intelligence (AI) to infer from the data the position of police patrols and sells that information to whomever is interested in knowing that position. Even if this is not prohibited under administrative or criminal law, it undermines the interest of the municipality and/or of other public entities to ensure effective police work and is thus in violation of paragraph (2) of this Principle.

REPORTERS' NOTES

United States:

The Open, Public, Electronic, and Necessary Government Data Act (also referred to in short form as the Open Government Data Act), enacted as part of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. 115-435, 132 Stat. 5529, contains rules governing access to data made available by the government of the United States. There is substantial variance at the state level in this regard. Although most U.S. states have some form of public data initiative, only 17 states have open data laws. See https://www.ncsl.org/research/telecommunications-and-information-technology/state-open-data-laws-and-policies.aspx. An additional four U.S. states have open data guidelines promulgated by executive order. See, e.g., https://www.governor.ny.gov/sites/default/files/atoms/files/EO95_0.pdf. New York's open data handbook is available at https://data.ny.gov/download/id8k-natf/application/pdf. Details of terms

of use vary as well. See, e.g., New York's terms of use, available at https://data.ny.gov/download/77gx-ii52/application/pdf.

Europe:

a. Freedom of use as the default rule and *b. Limitations on freedom of use.* Initiatives to ensure general accessibility of public data have been discussed at a European policy level for over two decades (see COM(1998) 585 final and Public Sector Information (PSI) Directive 2003/98/EC). The underlying rationale is that government data is an untapped resource for innovative products and services that has been produced with public money. Therefore, the data should be publicly available and used for the benefit of society. With the Open Data Directive (Directive (EU) 2019/1024), the European legislator renewed its open data efforts and introduced new rules to facilitate the reuse of data held by the public sector. An additional set of provisions for the reuse of specifically protected data held by public bodies (such as personal data), which is largely excluded from the scope of the Open Data Directive, can now be found in the Data Governance Act (Regulation (EU) 2022/868). The notion that public data should be open by default is not only promoted by the European Union but has, for example, also been recommended by the Organisation for Economic Co-operation and Development (OECD). To maximize the use and reuse of public data, member countries should assume openness in public sector information as a default rule wherever possible. Grounds for limitations of this principle may be the protection of national security interests, personal privacy, or the preservation of private interests, for example, when protected by copyright (OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, 2008). Similarly, in the G8 Open Data Charter, the members of the G8 declared that free access to, and subsequent reuse of, public data are of significant value to society and the economy. They agreed to orient their governments toward open data by default while recognizing that there are legitimate reasons, such as intellectual property and data protection law, that may restrict the sharing of data. Further, they agreed that data should be available free of charge in order to encourage its most widespread use, and be released in open formats whenever possible, to ensure that the data is available to the widest range of users for the widest range of purposes. In a similar vein, Principle 1 of the International Open Data Charter, a collaboration between over 100 governments and organizations, states that there should be a presumption of publication for government data and that governments should justify data that is kept closed, for example for security or data protection reasons.

While the data openness debate was for a long time primarily focused on public data, facilitating the exchange of data has also become a policy objective for business-to-business (B2B) relations. With markets becoming more and more data-driven, having access to data may not only determine economic success in the digital age but also create innovative services and products, reduce costs, and improve efficiency. Triggered by new technological developments, such as "Internet of Things" (IoT) and artificial intelligence (AI), openness of data in the private sector has moved to the center of European policy discussions. It is, however, recognized that open data, the most extreme approach to data openness, may be less fitting for privately held data than for public data, and thus different considerations need to be taken into account. (OECD, Enhancing Access to and Sharing of Data: Reconciling risks and benefits of data re-use, 2019). Given the potential

benefits of data openness, the European Commission has set out to create a framework that enhances the data flow between businesses. A first step in that direction has been taken by the Data Governance Act, which not only contains rules on the reuse of public data but also proposes provisions to facilitate the sharing of data among businesses.

The data exchange between businesses and governments (business-to-government (B2G)) is guided by the principle of "purpose limitation" (or "data-use limitation") (COM(2018) 232 final, p. 13). That principle states that the use of private sector data should be clearly limited to one or more purposes to be specified as clearly as possible in the contractual provisions that establish the B2G collaboration. Those may include a limitation of duration for the use of the data. Furthermore, the private sector entity should receive specific assurances that the data obtained will not be used for unrelated administrative or judicial procedures. The High-Level Expert Group (HLEG) on B2G Data Sharing essentially upheld the core tenet of that principle, but proposed to clarify that the public sector should be able to combine the private-sector data with data from other sources. Furthermore, it was suggested to change the term to "data-use limitation" because "purpose limitation" is primarily used in a privacy law context (HLEG on B2G Data Sharing, Towards a European strategy on business-to-government data sharing for the public interest, 2020). The Chapter of the Data Act proposal (COM(2022) 68 final) on B2G data sharing is also based on the principle of "purpose limitation." In cases of "exceptional need" a public body or a Union institution, agency, or body may access privately held data (Article 14 Data Act proposal). The public body may not use that data in a manner incompatible with the purpose for which the data were requested (Article 19(a)). In addition, technical and organizational measures that safeguard the rights and freedoms of data subjects have to be implemented (Article 19(b)) and the data has to be destroyed as soon as it is no longer necessary for the stated purpose (Article 19(c)).

By recommending that data may be used for any lawful purpose and in any lawful way, unless it is explicitly agreed or stated otherwise or inconsistent with the purpose for which the right had originally been afforded, this Principle follows the general trend of promoting data openness in the B2B sector in order to help foster innovation and growth. This is also consistent with the approach taken by Articles 4 and 5 of the Data Act proposal, which allow the user to access and share all the data generated by the use of an IoT product or related service but restrict certain use that would be inconsistent with the purpose for which the rights were afforded (see the Reporters' Notes to Principle 20).

c. No-harm principle. The meaning of the "no-harm" principle formulated in paragraph (2) does not correspond with that of the "do no harm" principle for B2G data sharing that has been put forward by the European Commission (COM(2018) 232 final, p. 13). The meaning the European Commission attached to the principle of "do no harm" is that B2G data collaborations must ensure that protected interests, such as trade secrets, are respected. While paragraph (2) of this Principle also concerns the protection of such interests, its scope is limited to the legitimate interests of the original controller and parties within that controller's sphere of interest. The interests of protected third parties are dealt with in Part IV of these Principles. The conflict in terminology between this Principle and the B2G principles of the European Commission might soon be resolved, as the HLEG on B2G data sharing suggested changing the "do no harm" principle to "risk mitigation and safeguards."

The Data Act proposal also provides for a rule that prohibits the person benefitting from an access or sharing right to use that data to cause harm to the original data holder. Articles 4 and 5 of the proposal give the user of an IoT product the right to access all the data generated by the use of the IoT product or to have the data shared with a third party. However, the user and third-party recipient must not use the obtained data to develop a product that competes with the product from which the data originate (Article 4(4) and Article 6(2)(c)). In addition, Article 6(2)(c) prohibits the third party from sharing the data with another third party, in raw, aggregated, or derived form, unless necessary to provide the service requested by the user. In all those scenarios, the use of the data by the user or the third party could potentially harm the legitimate interests of the original controller beyond what is inherent in the purpose for which the data access and sharing rights were introduced.

Principle 27. Reciprocity

If the law affords a data access right within the meaning of Principle 24 to a party against a controller, this is a strong argument for affording a similar data access right to the original controller against the first party under comparable circumstances. Whether this argument should prevail depends, among other things, on whether affording such a reciprocal right would be inconsistent with the purpose of provision of access to the first party.

Comment:

a. Reciprocity. This Principle is a very "soft" Principle, reflecting basic notions of fundamental fairness and giving some—necessarily general—guidance as to their possible implementation. Generally speaking, notions of fairness require a certain degree of reciprocity, i.e., if a party benefits from receiving data under a data sharing regime for the public interest, that party should normally be prepared to share similar data under similar conditions with the controller that had originally shared the data. This may often be achieved by simply formulating the scope of the relevant law in a way that it imposes the same duties on the recipient.

Illustration:

122. In a situation such as that in Illustration no. 118, research institute R2 should normally be subject to the same open research data regime as R1. As a result, next time it may be R1 that profits from data published by R2.

In many situations, however, more sophisticated steps may need to be taken in order to provide for reciprocity, e.g., because the original controller and the receiving party are very different and not subject to the same rules.

Illustration:

123. The law provides that a municipality must share, for free, mobility data from smart road infrastructure with whoever is interested in the data. When designing the law, the legislator might wish to consider including a duty on recipients that gain valuable insights from this data, e.g., about traffic flows in the city, to share this derived or inferred data with the municipality.

Naturally, reciprocity is not called for when the purpose for which the access right within the meaning of Principle 24 was originally afforded is inconsistent with reciprocity, such as when the data access right was afforded under some state's domestic law in order to balance an initially imbalanced market position of the parties.

Illustration:

124. If the law provides for a data sharing obligation for large platforms for the benefit of micro-, small-, and medium-sized enterprises (MSMEs) trying to enter the market, it would obviously undermine the purpose of that law if, conversely, and relying on the notion of reciprocity, the large platforms could exercise a data access right against the MSMEs.

REPORTERS' NOTES

United States:

For a discussion of reciprocity in data sharing systems, see, e.g., Inst. of Int'l Fin., Reciprocity in Customer Data Sharing Frameworks (July 2018), available at https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf. See also Cong. Rsch. Serv., Cross-Border Data Sharing Under the CLOUD Act (2018); Virginia A. de Wolf, Joan E. Sieber, Philip M. Steel & Alvan O. Zarate, *Part I: What Is the Requirement for Data Sharing?*, 27(6) IRB: ETHICS & HUM. RSCH. 12-16 (2005), doi:10.2307/3563537.

Europe:

In European legislation on data sharing, an explicit reference to the notion of reciprocity can be found in the Infrastructure for Spatial Information in the European Community (INSPIRE)

Directive (Directive 2007/2/EC). Article 17 of the INSPIRE Directive provides rules for the sharing of spatial data between public authorities of Member States for the purposes of public tasks that may have an impact on the environment. Any restrictions likely to create practical obstacles to the sharing of spatial data sets and services are precluded. Charging fees for and licensing of the spatial data remains possible, but should be kept to the minimum required to ensure the necessary quality and supply of spatial data sets and services together with a reasonable return on investment. The INSPIRE Directive explicitly stipulates that, on the basis of reciprocity and equivalence, the data sharing regime put forward by Article 17(1) to (3) shall also be open to bodies established by international agreements to which the EU and Member States are parties.

Another explicit reference to the principle of reciprocity in data exchanges can be found in connection with ambient air data. In an Implementing Decision, the European Commission lays down rules for the reciprocal exchange of ambient air quality data between Member States, in order to establish a sound informational basis for measures to reduce air pollution (Commission Implementing Decision 2011/850/EU OJ L 2011/335, p 86).

The idea underlying this Principle is already, to some extent, present in patent law. The predominant example is Article 31 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which addresses other use without authorization of the right holder and sets out in its paragraph (l) that when such use is authorized to permit the exploitation of a patent ("the second patent") that cannot be exploited without infringing another patent ("the first patent"), the owner of the first patent shall be entitled to a cross-license on reasonable terms to use the invention claimed in the second patent (see also Section 24(2) German Patent Act). In addition, the typical fair, reasonable, and non-discriminatory (FRAND) declarations on standard-essential patents offer the holder the option of granting a FRAND license only on the condition of reciprocity (see European Telecommunications Standards Institute (ETSI) Intellectual Property Rights Policy para 6.1).

PART IV
THIRD PARTY ASPECTS OF DATA ACTIVITIES

CHAPTER A
PROTECTION OF OTHERS AGAINST DATA ACTIVITIES

Principle 28. Wrongfulness of Data Activities vis-à-vis Another Party

(1) Data activities are wrongful vis-à-vis another party (a "protected party") if:

(a) they violate any right of the protected party that has third-party effect per se within the meaning of Principle 29;

(b) they do not comply with contractual limitations on data activities, enforceable by the protected party, of the sort described in Principle 30; or

(c) access to the data has been obtained from the protected party by unauthorized means within the meaning of Principle 31.

(2) In assessing whether data activities are wrongful, the conditions under which these activities are pursued, such as provision of an adequate level of data security or compliance with any duty under Principle 32, should be taken into account.

(3) Implementation of this rule should take into account applicable doctrines of justification, such as freedom of information and expression.

Comment:

a. General observations. Previous Parts of these Principles have focused on legal relationships that are essentially bilateral in nature. Even when contracts are of a type that is usually concluded among multiple parties, such as data pooling arrangements, the relevant Principles in Part II have focused on the relationship among the contracting parties. Likewise, even when data rights are of a type usually exercised by many parties in parallel, such as rights to receive an economic share in profits derived, the relevant Principles in Part III have focused on the relationship between a party exercising a data right and the controller against whom the right is exercised. Rights and legitimate interests of third parties play a role, of course, such as with regard to certain due diligence and data security obligations (e.g., Principle 7(2)(c)(iv)), or in the context of the factors that need to be assessed when deciding whether or not to grant a data right (e.g., Principle 19(2)(c)), and if so, which specifications should be made and which protective measures for the benefit of affected parties should be taken (e.g., Principle 19(3)). However, in those contexts

the legitimate interests of affected parties were considered as factors to be taken into account within a wider balancing exercise, not as rights that those affected (third) parties might themselves enforce against the contracting parties or the party exercising a data right and the controller.

This is where Part IV comes into play. Chapter A of Part IV gives guidance to courts and legislators as to when data activities should be considered wrongful vis-à-vis another party, be that a third party or even a contracting party (as a contracting party may, when data is passed on in a chain of transactions, become a third party with regard to a downstream transaction). The term "data activities" is defined very broadly and covers any activity with regard to data, including acquisition, control, processing or use, and onward supply. While Chapter A sets out the general grounds for wrongfulness vis-à-vis a protected party, Chapter B more specifically deals with the situation of onward supply of data and the effects such onward supply may have on the protection of affected parties. In this context, Chapter B not only states duties for the onward supply of data (Principle 32), but also sets out conditions under which an initial supplier may take direct action against a downstream recipient (Principle 33), and the conditions under which wrongful activities on the part of a supplier also make the activities of a downstream recipient wrongful (Principle 34). Chapter C addresses similar issues in the context of processing of data.

This Principle is of an introductory nature. It sets out three grounds of wrongfulness of data activities that are described in more detail in Principles 29 to 31. The list provided in paragraph (1) of this Principle is not exhaustive, i.e., there are other reasons why an activity with regard to data may be wrongful, the most obvious being that it violates law other than law referred to in Principles 29 to 31 or is generally in breach of contract, in particular a contract described in Part II. Of course, as stated in Principle 1(2), nothing in Principles 28 to 37 is intended to amend or create data privacy or data protection law, intellectual property law, or trade secret law, so if any of these bodies of law provides for different or more specific solutions for the issues addressed in Part IV, those solutions take priority.

b. Grounds of wrongfulness. There are three cases in which a data activity is considered to be wrongful under the nonexhaustive list in paragraph (1). The first case is interference with any right within the meaning of Principle 29, i.e., intellectual property rights or personality rights such as data privacy/protection rights.

Illustration:

125. Provider B of a video game processes user data covered by a data protection regime that requires, for processing to be lawful, the users' consent. If B processes the data without such consent, these data activities are wrongful vis-à-vis the data subjects within the meaning of paragraph (1)(a) of this Principle and Principle 29.

The second case is noncompliance with contractual limitations within the meaning of Principle 30. While the breach of any contractual duty may give rise to remedies under applicable law, it is more specifically the breach of a contractual duty limiting data activities that leads to wrongfulness under paragraph (1)(b) of this Principle. Such contractual limitations not only lead to wrongfulness vis-à-vis the contracting partner, but may also, under the conditions set out in Principle 34, take effect vis-à-vis a downstream recipient.

Illustrations:

126. Controller C of valuable sensor data entrusts the data to processor P. The contract with P contains a clause according to which P may not pass the data on to any third party. If P, in violation of that clause, passes the data on to T, this data activity of P is wrongful vis-à-vis C under paragraph (1)(b) of this Principle and Principle 30. Whether T is also acting wrongfully depends on Principle 34.

127. Controller C in Illustration no. 126 sells the sensor data to business B under a contract. The data is immediately transferred to B, and B is under an obligation to pay the purchase price in several installments. After B has failed to pay two installments despite reminders, C terminates the contract. B is clearly in breach of contract, and after termination of the contract B must erase the data (but see Principle 4(2)) and may no longer use it, but this is not the kind of "contractual limitation" addressed by paragraph (1)(b) of this Principle and Principle 30.

Finally, data activities are wrongful according to paragraph (1)(c) of this Principle if data has been obtained by unauthorized means within the meaning of Principle 31. This concerns primarily the relationship between the person that obtained the data by unauthorized means and the initial controller (from which this person obtained the data). Whether this ground of wrongfulness also takes effect against a downstream recipient is determined by Principle 34.

Illustration:

128. Hacker H hacks B's servers in Illustration no. 125 and thus obtains access to the user data. This is a wrongful data activity under paragraph (1)(c) of this Principle and Principle 31. If H passes the data on to T, the question of whether T is also acting wrongfully is a question of Principle 34.

c. Data security and other additional standards. Paragraph (2) clarifies that rightfulness of data activities is not just a matter of whether control, a particular form of processing, or onward supply is rightful as such, but also a matter of how it takes place. A particularly important requirement is that of providing an adequate level of data security. It is beyond the scope of these Principles to define which technical measures need to be taken, and what qualifies as an adequate level of security. These determinations can be made in specific legislation or industry standards, or, in their absence, be reached by courts relying on general doctrines and principles considering the weight of the rights of third parties that are at stake, the magnitude of the risk of data breaches occurring, and the gravity of the potential consequences. Failure to comply with these requirements makes the data activities wrongful.

Illustration:

129. If B in Illustration no. 125 has obtained the users' consent but fails to apply basic data security measures when storing the data, storage of the data (as a type of data activity) may be wrongful vis-à-vis the data subjects.

Apart from the requirement to provide an adequate level of data security, there may be a host of other requirements, such as requirements under applicable rules of public law, and of course any duty to be complied with in the context of onward transfer under Principle 32.

d. Justifications. As this Principle is largely founded on a tort-law logic, due account must be taken of possible grounds of justification. One example would be freedom of the press, such as when investigative journalists obtain control of particular data.

Illustration:

130. Journalist J receives bank account data proving that politician P has misappropriated public funds. Even if J has notice that this data has been acquired either in breach of contract or by unauthorized means, J's own data activities may exceptionally be justified and therefore not wrongful according to paragraph (3) of this Principle.

REPORTERS' NOTES

United States:

There are many circumstances under U.S. contract law in which an action that is in breach of contract as between the parties is wrongful with respect to a third party, who then has redress for that breach. Sometimes, the circumstances are provided for by statute. See, e.g., Uniform Commercial Code § 2-318 (2021-2022 ed.), providing that a seller's warranty extends to certain third parties. Other times, common-law doctrines, particularly those relating to third-party beneficiaries, bring about a similar result. See generally Restatement of the Law Second, Contracts, Chapter 14 (AM. L. INST. 1981).

Third-party effects in tort law can be seen, inter alia, in the field of products liability. See, e.g., Restatement of the Law Third, Torts: Products Liability § 1 (AM. L. INST. 1998).

See also Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323 (2004).

Europe:

a. General observations. In EU law, a line is drawn between rights that can only be enforced against a certain party ("*inter partes* rights," "relative rights") and rights that can be enforced against everybody ("*erga omnes* rights," "absolute rights," or "rights with third-party effects"). The most prominent example for the former is a right arising out of a contractual relationship. As a general rule, third parties cannot acquire rights from the contract, nor are they obligated to adhere to the obligations stated in the contract, as the contractual relationship only produces effect for the contracting parties. The relative effect of contractual rights is a central notion in European contract law and is explicitly stated in Article 1165 of the French Code Civil, which articulates that "agreements produce effect only between the contractual parties." However, there are some exceptions to that general rule. For example, it is prohibited to deliberately induce a person not to fulfill the person's contractual obligations toward the other party to the contract. In such circumstances, the person inducing the non-performance may be considered as committing a tort/delict (see Article VI – 2:211 DCFR; Article 2:211 Principles of European Law – Non-Contractual Liability Arising out of Damage Caused to Another (PEL Liab. Dam.); Reporters' Notes to Principle 34). Absolute rights, on the other hand, can be enforced against any third party. The most relevant examples of such rights with regard to data can be found in copyright law, the *sui generis* protection of databases, and in the General Data Protection Regulation (GDPR) (see the Reporters' Notes to Principle 29).

b. Grounds of wrongfulness. The grounds of wrongfulness draw some inspiration from the Trade Secrets Directive (Directive (EU) 2016/943), under which the use or disclosure of a trade secret is considered unlawful if carried out by a person who unlawfully acquired the trade secret, or is in breach of a confidentiality agreement, contractual duty, or any other duty that limits its disclosure or use (Article 4(3) Trade Secrets Directive). The acquisition of a trade secret without the consent of the trade secret holder is considered unlawful, whenever carried out by unauthorized access to, appropriation of, or copying of any documents, objects, materials, substances, or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or

from which the trade secret can be deduced. Furthermore, the acquisition of a trade secret is unlawful if it is carried out by any other conduct that, under the circumstances, is considered contrary to honest commercial practices (Article 4(2) Trade Secrets Directive). The protection under the Trade Secrets Directive is nearly identical to the protection of undisclosed information in Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) between all the member nations of the World Trade Organization (WTO).

Implicitly, the three grounds of wrongfulness can also be found in the Data Act proposal, even though the Data Act proposal does not put forward a set of provisions dealing with the wrongfulness of data activities vis-à-vis another party. Several provisions in the Data Act address interferences with rights of protected parties that have third-party effects. When the user of an "Internet of Things" (IoT) product exercises its right to access the data generated by the use of the IoT product, any personal data relating to a natural person that is not the user shall only be made available by the data holder to the user when there is a valid legal basis under the GDPR (Article 4(5); see also Article 5(6)). Moreover, according to Article 4(3), trade secrets shall only be disclosed provided that all specific, necessary measures are taken to preserve the confidentiality of trade secrets, in particular with respect to third parties (see also Article 5(8)). The Member States have to lay down rules on penalties applicable to infringements of the Data Act proposal (Article 33). Regarding contractual limitations, Article 4(6) stipulates that the data holder shall only use non-personal data generated by the use of an IoT product or related service on the basis of a contractual agreement with users of the IoT product. Additionally, Article 8(2) provides that the data holder shall agree with a data recipient on the terms for making the data available. It follows from those two provisions and the general rules of contract law that any data activities that violate the agreement between the data holder and the recipient would be an infringement of the Data Act proposal that trigger penalties under the national law of the Member State. Finally, in a case in which the recipient abused evident gaps in the technical infrastructure of the data holder designed to protect the data, the recipient has to destroy the data made available by the data holder and any copies thereof (Article 11(2)(a)). In addition, the recipient has to end the production, offering, placing on the market, or use of goods, derivative data, or services produced on the basis of knowledge obtained through such data, or the importation, export, or storage of infringing goods for those purposes, and destroy any infringing goods (Article 11(2)(b)).

c. Data security and other additional standards. The GDPR (Regulation (EU) 2016/679) qualifies processing in a manner that ensures appropriate security of the personal data as one of the guiding principles relating to processing of personal data (see Article 5(1)(f) GDPR). This includes the protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage by using appropriate technical or organizational measures. Also, in assessing whether processing of data for secondary purposes according to Article 6(4) of the GDPR is lawful, account must be taken of the existence of appropriate safeguards for both the original and intended further processing (see also Recital 50 GDPR). Finally, a high level of security for the storage and transmission of non-personal data is also a condition for providing a data intermediation service in the Data Governance Act (DGA) (Regulation (EU) 2022/868, Article 12(l)). The failure to comply with the conditions in the DGA can lead to financial penalties or even the forced cessation of the data intermediation service.

The standards for cybersecurity and network and information security are currently being developed all around the world (for an overview, see European Commission, Rolling Plan for ICT Standardisation, 2020, p. 34 ff.). This includes work from international standardization agencies such as the European Committee for Standardization and the European Committee for Electrotechnical Standardization (CEN CENELEC) Joint Technical Committee on 'Cybersecurity and data protection' (CEN-CLC/JTC 13) and the European Telecommunications Standards Institute (ETSI), e.g., in the Technical Committee Cyber (TC Cyber). On a European level, the European Union Agency for Cybersecurity (ENISA) drafted a candidate cybersecurity certification scheme on the basis of the Cybersecurity Act. Furthermore, the International Organisation for Standardisation (ISO) works on several areas of information security and cybersecurity in its Sub Committee 27 (SC 27, see https://www.iso.org/committee/45306.html). Further initiatives are pursued by the International Telecommunications Union and the Internet Engineering Task Force (IETF).

d. Justification. Under tort law, liability is excluded if the defendant's actions are justified. Examples of widely recognized grounds of justification can be found, for example, in the Principles of European Tort Law (PETL): the defendant acts in self-defense, under necessity, because the help of the authorities could not be obtained in time (self-help), with the consent of the victim, or by virtue of lawful authority (cf. Art. 7:101 PETL). Those defenses are also laid down in Chapter 5, Book VI, of the Draft Common Frame of Reference (DCFR) and the Principles of European Law (PEL).

Liability under the Trade Secrets Directive is excluded when the alleged acquisition, use, or disclosure of the trade secret was carried out (a) to exercise the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media; (b) to reveal misconduct, wrongdoing, or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest; (c) by workers for their representatives as part of the legitimate exercise by those representatives of their functions in accordance with EU or national law, provided that such disclosure was necessary for that exercise; and (d) for the purpose of protecting a legitimate interest recognized by EU or national law. However, the broader formulation chosen in paragraph (3) of this Principle provides a more flexible approach that allows for new grounds for justification that may arise in the future.

The GDPR leaves the relationship between the right to the protection of personal data and the right to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes, to the law of the Member States. Member States shall provide for exemptions or derogations if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information (Article 85).

Principle 29. Rights that Have Third-Party Effect Per Se

(1) For the purpose of Principle 28(1)(a), rights that have third-party effect per se include the following:

(a) intellectual property rights and similar rights;

(b) data privacy/data protection rights and similar rights; and

(c) any other rights that, under the applicable law, have similar third-party effects.

(2) The extent to which rights within the meaning of paragraph (1) limit data activities, as well as the effect of such limitations, is determined by the applicable law.

Comment:

a. Traditional erga omnes *rights.* This Principle provides a nonexhaustive list of rights that take effect against any third party (*erga omnes*), as contrasted with rights that take effect only against a particular party (*inter partes*). What is special about the rights listed in this Principle (compared, e.g., with entitlements following from situations described in Principle 30 or 31) is that these rights have third-party effect per se; others have to respect them per se; and infringements are normally wrongful, subject to justification, without additional elements such as bad faith (even though the applicable national law may, of course, impose such additional elements as conditions for the availability of remedies for infringement).

Rights that take effect against any third party in this way include intellectual property rights (paragraph (1)(a)), such as patent protection or copyright protection, including protection for computer programs. Data may be protected by such intellectual property rights, but not all data is protected by intellectual property rights, and, in fact, most data is probably not. Apart from intellectual property rights, there are also a number of rights that are closely related to intellectual property rights because they work in a similar manner. An example for such a related right would be the European *sui generis* database right under Directive 96/9/EC, which is a particular form of investment protection.

Besides intellectual property rights, there are a number of entitlements with regard to data that do have third-party effect but work in a different manner. This concerns, in particular, personality rights, which are the basis of data privacy/data protection rights under a number of legal regimes (paragraph (1)(b)). The extent to which such rights are vindicated under the relevant legal regimes by way of public enforcement or private enforcement is not determinative, as long as the basis for public enforcement is still the protection of particular parties (as contrasted with, for example, the market).

Illustration:

131. A U.S. state adopts by law a data privacy regime that does not provide for rights that individual data subjects, or a class of data subjects collectively, can exercise and enforce in court, but that provides only the basis for state authorities to take action against a business. Provided the law is introduced to protect data subjects, the protection thus afforded still potentially qualifies as a "right" within the meaning of this Principle. If, however, the rationale is the regulation of data markets, that falls outside the scope of this Principle.

Paragraph (1) of this Principle is not exhaustive. Rather, subparagraphs (a) and (b) list two types of rights that have third-party effects, while subparagraph (c) leaves room for rights that, under the applicable law, have similar third-party effects. A third-party effect can be considered "similar" if, by effect of law, any third party interfering with the right might face remedies and other sanctions. This will often include trade secrets, which are not intellectual property, but which, due to a separate body of law affording protection, provide their holder with a kind of "soft intellectual property protection." Whether or not this is the case under the applicable law depends, in particular, on whether or not a third party buying a trade secret in good faith from a person who acquired it in unlawful ways may face remedies for the benefit of the original holder.

Illustration:

132. Before Directive (EU) 2016/943, trade secrets law in some European jurisdictions was more or less pure tort law. If H unlawfully stole one of C's trade secrets and sold it to T, who acted in good faith, only H would have been a tortfeasor, but not T. This would not have been an effect "similar" to intellectual property protection. Since the implementation of the Directive, trade secrets also take effect against third parties who acquired the trade secret in good faith from a person who acquired it unlawfully, if the third party later becomes aware of those facts. So, trade secrets in the European Union can now be considered as affording their rightful holder a "similar" right within the meaning of paragraph (1)(c) of this Principle.

b. A general data ownership right? There has been much discussion about whether there is such a thing as "ownership" in data, and if so, what it would mean. There can be little doubt that information as such is not subject to "ownership" but is normally free in the absence of specific

doctrines, such as trade secret law, that restrict rights with respect to it. Data, as the term is used in these Principles, is different from information, in that it is information recorded on a medium and typically expressed in code (such as a characteristic binary string of 0 and 1). Legal regimes have recognized this difference in a number of ways, such as by giving greater rights to control access to data than to control access to information. Whether data can constitute "property" that can be "owned" is a topic that is subject of debate. After all, while data (or control of it) can have economic value, data is a non-rivalrous resource that can be duplicated or multiplied at basically no cost, making it different in important ways from traditional forms of property. These Principles take no position as to whether data constitutes "property" that can be "owned," but if a legal system introduced such an ownership right, and if it had third-party effects per se, it would be subsumed under paragraphs (1)(c) or (1)(a) of this Principle, depending on the nature of the right in the relevant legal system.

c. Effects governed by the applicable law. Paragraph (2) of this Principle clarifies that, even though the rights mentioned in this Principle have third-party effect per se, this holds true only for the "core right" as such, whereas the exact extent to which rights within the meaning of paragraph (1) limit data activities, as well as the effect of such limitations, is determined by the applicable law. While other *erga omnes* rights, such as ownership in tangible property or health and bodily integrity of a natural person, normally enjoy quite comprehensive protection against all sorts of interference, other *erga omnes* rights, including the rights listed in this Principle, are normally more limited and afford protection only against a defined range of activities.

Illustration:

133. C holds the copyright in large amounts of text data. P uses the copyright-protected material, which is accessible online, intended for human readers, for training AI (so-called text and data mining (TDM)). Training the AI on the text does not automatically interfere with C's copyright; it interferes with C's copyright only if training AI is generally among the activities that the holder of copyright is entitled to control and if no exception from copyright protection applies. Thus, the question whether the data activities pursued by P are wrongful vis-à-vis C cannot be answered without an in-depth analysis of the content and limits of copyright protection under the applicable law.

Given that the degree and form of protection varies from jurisdiction to jurisdiction, the question whether or not a data activity is wrongful vis-à-vis the holder of a right within the meaning of this Principle depends on which jurisdiction's law applies in the individual case.

REPORTERS' NOTES

United States:

The distinction between rights effective only between parties in privity with each other and those that are effective against third parties is well known in the United States. In the law of secured transactions, for example, the requirements for a security interest that is enforceable (i.e., effective only [with few exceptions] between the parties) and one that is perfected (effective against third parties) differ. See Uniform Commercial Code §§ 9-203 and 9-308 (2021-2022 ed.). The distinction is recognized not only in the common-law states but also in Louisiana, which is a civil-law state. See, e.g., the discussion of the distinction in the context of assignment and subrogation in 5 SAUL LITVINOFF, THE LAW OF OBLIGATIONS IN THE LOUISIANA JURISPRUDENCE § 11.32, at 283 (1992): "subrogation is effective against third persons, including the obligor, from the time it takes place, which is expressed by saying that it produces effects erga omnes, while an assignment of rights requires notice to the debtor or his express acceptance in order to be effective against third persons."

With respect to issues relating to data privacy and data ownership, see the developing concept of information fiduciaries. In this regard, see, e.g., Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/L277-CZLG]; Jack M. Balkin, *Lecture, Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016). For a contrasting view, see Lina Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

Europe:

a. Traditional erga omnes rights.

(i). *Copyright*. Besides ownership, copyright is one of the most important rights with third-party effects. European copyright law has been harmonized by the Information Society Service Directive (Directive 2001/29/EC), which has recently been amended by the Copyright Digital Single Market (DSM) Directive (Directive (EU) 2019/790). In addition, the European Union has adopted a number of specific instruments in the field, such as the Database Directive (Directive 96/9/EC) and the Software Directive (Directive 2009/24/EC). The European legal framework on copyright does not provide for a list of types of protected works, as the Berne Convention does. In principle, any type of work can enjoy copyright protection as long as it meets the legal requirements that the work is an expression of an idea that manifests itself in some material or concrete form and is "original." Those requirements are explicitly stated in the Software Directive, which protects computer programs by copyright as literary works. Excluded from the scope are ideas and principles that underlie any element of a computer program (Article 1(2) of the

Software Directive). The protection of a "computer program" requires that it is original in the sense that it is the author's own intellectual creation (Article 1(3) Software Directive). According to the still prevailing view, the "author" must be human, and a machine, even if powered by advanced artificial intelligence (AI), would not suffice. Data that is measured by sensors or produced by machines could therefore only be covered if the design of the data can directly be traced back to the software designer (Andreas Wiebe, Protection of industrial data – a new property right for the digital economy, 2016 *Gewerblicher Rechtsschutz und Urheberrecht International*, p. 877, 879). However, the European Parliament has recently taken the view that technical creations generated by AI technology must be protected under intellectual property law in order to encourage investment and improve legal certainty for citizens, businesses, and inventors (European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI), P9_TA(2020)0277, No. 15). The Parliament called on the Commission to support common, uniform copyright provisions applicable to AI-generated works in the Union for cases in which such works could be eligible for copyright protection (*ibid*, No. 15).

The Database Directive establishes a legal framework for two types of intellectual property rights relating to databases. First, the Directive clarifies in Article 3(1) that databases can qualify for copyright protection if they satisfy the creativity and originality criterion that applies to any other copyright protected work. Second, the Directive introduces a *sui generis* protection for databases, if the maker "shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database." However, the scope of the database protection is very limited. According to the British Horseracing (Case C-203/02 ECLI:EU:E:2004:695 – *British Horseracing*) and Fixtures Marketing (Case C-46/02 ECLI:EU:C:2004:694 – *Fixtures Marketing*) judgments of the Court of Justice of the European Union (CJEU), the Directive does not protect investments in the creation of new data but only the identification and collection of existing material. Therefore, investments in data creation are excluded from the scope of the *sui generis* right. Due to this limitation in scope, data producers will often fail to meet the requirements to qualify as creators of a database. However, especially when data is generated by connected devices, the differentiation between the creation of new data and the collection of existing data may not always be clear. In the *Autobahnmaut* case (Case I ZR 47/08 – *Autobahnmaut*), the German Supreme Court held that the private company Toll Collect has a *sui generis* right in the dynamic database used for billing the individual operators. The German Supreme Court argued that the data registered by the terminals and vehicles was not "created" by Toll Collect but existed independently of the investment made by the database maker.

(ii). *Data privacy*. The protection of personal data is a fundamental right protected by the Article 8 of the Charter of Fundamental Rights of the European Union. Furthermore, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) provides for an extensive protection of personal data against any infringements, including by third parties. The Regulation defines "personal data" broadly as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or

indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4(1) GDPR). This broad concept renders it rather difficult for those responsible for anonymizing personal data, and thus escaping the protection regime of the GDPR. The processing of personal data is only lawful if it is justified by one of the grounds listed in Article 6, or, for more sensitive categories of data (such as health data), in Article 9.

The E-Privacy Directive (Directive 2002/58/EC) provides the basic legal framework for data protection in electronic communications. Currently, a revision of the E-Privacy Directive is being discussed at the EU level (COM(2017), 10 final). Most recently, a Presidency discussion paper of the Proposal was published (ST 9931 2020 INIT). However, due to many unresolved points of contention, it is as yet uncertain whether a new Regulation will be adopted, and what policy choices will be made.

(iii). Trade secrets. Third-party effects may also arise from the Trade Secrets Directive. A "trade secret" is defined as information that meets the following requirements: (a) it is secret in that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; and (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. The definition of a "trade secret" is almost identical to that of the protection of undisclosed information in Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). According to Article 39(2), natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information: (a) is secret in that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. However, the Trade Secrets Directive does not grant an exclusive right to data as such, because the protection under the Directive depends on the factual existence of a secret and is thus more similar to the protection of possession. Furthermore, the trade secret is not protected against any kind of use, but only against certain forms of infringement under Article 4 of the Directive (see Herbert Zech, 'Information as a tradable commodity', in: De Franceschi (ed.), European Contract Law and the Digital Single Market, 2016, p. 51, 63 f.).

b. A general data ownership right? Finally, there has been a lively debate about "data ownership" in Europe. The debate may originally have been sparked in Germany, fueled by the automobile and other industries worrying about the protection of "Internet of Things" (IoT) data they accumulate and by the consumers' desire to participate more in the profits made by the data economy. After the European Commission mentioned the option of introducing a "data producer's right" at the EU level in its Communication on Building a European Data Economy (COM(2017) 9 final, p. 10 ff.), the debate spread throughout Europe. It soon became more or less common

opinion, however, that the concept of exclusive ownership rights in data that might be comparable to ownership in tangible property or to intellectual property rights is not a good way forward (see Opinion of the Data Ethics Commission, 2019, p. 104 f.). It is commonly held that such a regime would have the potential of suffocating the European data economy rather than boosting it, and given that consumers would readily contract away their ownership, very much as they are currently contracting away any other rights they have with regard to data, this is not likely to enhance consumer rights either (Maartje Elshout et al., Study for the European Commission on consumer's attitudes towards terms and conditions, 2016, p. 9; Jonathan A. Obar and Anne Oeldorf-Hrisch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, (2018) 22 iCS 1). The predominant view in Europe currently is that access rights and similar data rights are the more promising way forward (COM(2022) 68 final p. 3; COM(2020) 66 final, p. 4 ff.; COM(2018) 232 final, p. 9; see also the Reporters' Notes to Principle 23).

Principle 30. Contractual Limitations

(1) For the purpose of Principle 28(1)(b), a contractual limitation on data activities is a contractual term that limits data activities of any party to the contract, including by limiting the use or onward transfer of data.

(2) In determining whether a contractual limitation on data activities is in conflict with mandatory rules of law that vindicate important public policies and those that protect parties from overreaching conduct or agreements, factors to be taken into account include whether the agreement:

(a) unduly limits the freedoms of a contracting party, taking into account, inter alia, comparable limits of intellectual property protection;

(b) unduly limits activities in the public interest; or

(c) has unjustified discriminatory or anti-competitive effects.

Comment:

a. Contractual protection as compared with intellectual property protection. According to Principle 28(1)(b), data activities are wrongful if they fail to comply with contractual limitations within the meaning of this Principle. In practice, contractual limitations, such as in data transactions of the type described in Part II are common and used to substitute for the often missing protection provided by intellectual property law. However, contractual protection works in a somewhat different manner.

Intellectual property rights create an exclusive right, to the extent provided under intellectual property law, on the part of the rightholder to exploit the economic potential of a particular intellectual achievement, either by using it directly or by licensing it to others. The same holds true, in principle, for intellectual property–like schemes of investment protection. As far as intellectual property protection is afforded by the law, no third party may use the same intellectual achievement except with the rightholder's permission under a license. A license may be granted under certain conditions, but there are limits, notably limits posed by the exhaustion principle (first sale doctrine), and there are certain types of fair use, whether or not exhaustively listed in statutes, that are typically open to every third party.

If data is not protected by intellectual property law or any similar scheme, as is the case with many collections of data that are neither computer programs nor literary works nor otherwise protected by copyright or a related right, this does not automatically mean that the controller must keep the data absolutely closed down and secret if it does not want the data to be freely available to everyone. Rather, if a party is in control of data, and is not under an obligation to share the data with others, that party can make an offer to particular other parties or to the public at large to use the data on the basis of particular terms that are essentially contractual in nature. Generally speaking and subject to contract and other doctrines that protect the public interest and contractual protections against overreaching and oppressive terms, those terms will be enforced.

Illustration:

134. Business Y operates a website on which customers can search through flight data of various airlines, compare prices, and, on payment of a commission, book a flight. Y obtains the necessary data to respond to an individual query by automated means, inter alia, from a dataset linked to the publicly accessible website of airline X. Access to that website presupposes that the visitor to the site effectively accepts the application of X's general terms and conditions by ticking a box to that effect. The terms include a clause reading "The use of automated systems or software to extract data from this website for commercial purposes is prohibited unless the third party has directly concluded a written license agreement with X." If Y ticks the box by automated means and uses X's website in breach of the terms, Y has breached its agreement with X and thus Y's data activities are wrongful under Principle 28(1)(b) and this Principle.

b. Limits of protection as between the contracting parties. This Principle does not address what is required to make a valid contract, or to effectively impose a contractual limitation on the other party. As to the first point of contract formation, this may, in practice, be particularly difficult to establish in cases of data harvesting (data scraping) when the data collected is, in principle, publicly accessible on websites. The difficulties are largely related to establishing meaningful assent, and the situation could be considered to be similar to the provision of unsolicited services.

Formation of contract apart, general contract law, or special categories of contract law (such as consumer contract law), are also relevant as far as the substantive validity of terms is concerned. For instance, terms may be held to be objectionable, such as under doctrines of unconscionability or unfairness (when applicable), and there may be concerns under other doctrines related to public policy. As such doctrines diverge across different legal systems, paragraph (2) provides some guidance as to the circumstances the law ought to consider in determining whether terms are objectionable. In particular, paragraph (2) mentions consideration of whether the agreement unduly limits the freedoms of a contracting party, limits activities in the public interest, or has unjustified discriminatory or anti-competitive effects.

Illustration:

135. Assume that, in Illustration no. 134, the clause used by airline X reads "Extraction of data from this website for the purpose of comparing our prices with prices of other airlines is prohibited." This clause might, depending on the context, be held to be objectionable because of its anti-competitive effects.

It is a matter of some controversy whether fair use, first sale doctrine, and similar limiting concepts limit only intellectual property rights or if they also limit the reach of contractual terms that might provide for additional restrictions beyond those imposed by intellectual property law or limit the reach of contractual restrictions imposed on data not protected by intellectual property law. These Principles are generally favorable to the view that contractual limitations should normally not go further than would be permitted by comparable intellectual property law regimes, but there should be some flexibility to allow for the consideration of all elements of the case.

Illustration:

136. State X's copyright regime does not permit rightholders to limit text and data mining (TDM) in published, copyright-protected material for purposes of public interest

research. C publishes data that is not copyright protected, which University U wants to use for TDM in a public-interest research context. Everyone who wants to access the data must accept terms and conditions according to which TDM is not permitted unless C grants a license for which the user is required to pay. While copyright law and its exceptions do not apply, a court would, when confronted with the question of whether C can force U into a license contract, take into account the fact that C would not be able to do so if the data were protected by copyright.

c. Downstream, third-party effects. Contractual protection generally has direct effect only between the parties to the transaction, which is a major limitation of contractual protection as compared with intellectual property protection. However, when limits imposed by contract are infringed, there may still be some third-party effect under Principle 34, which provides that, when a downstream recipient had notice within the meaning of that Principle and the further requirements are met, contractual limitations may also be invoked against a downstream recipient.

REPORTERS' NOTES

United States:

In ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), the Seventh Circuit held that the defendant was bound by the license agreement for "shrinkwrapped" software because he had a chance to return the software after reading the license, including a provision limiting use of data to noncommercial purposes. A key question in that and subsequent cases was whether there was sufficient notice of the terms of use. In Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002), the Second Circuit held that there was insufficient notice of the terms of service, and thus the download of the software was not governed by an enforceable arbitration agreement. In Register.com v. Verio, 356 F.3d 3936 (2d Cir. 2004), the Second Circuit held enforceable a website's terms of service against a data-scraping bot that seemed to have violated those terms, on the ground that there was adequate notice of those terms. In MDY Industries, LLC v. Blizzard Entertainment, Inc., 629 F.3d 928 (9th Cir. 2010), as amended on denial of reh'g (Feb. 17, 2011), opinion amended and superseded on denial of reh'g, No. 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011), the Ninth Circuit held that a computer game player's violation of a game's terms of use by use of a bot could be actionable under contract law. In the case of hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019), the Ninth Circuit held that LinkedIn could be liable for tortious interference with hiQ's contracts with third parties when LinkedIn sought to prevent hiQ's bots from downloading public, nonproprietary data from LinkedIn's website.

With respect to the possibility of extending exclusive rights by contract when they are no longer available through intellectual property law, see, e.g., Impression Prod., Inc. v. Lexmark Int'l,

Inc., 137 S. Ct. 1523 (2017). See also Nancy S. Kim, *Revisiting the License v. Sale Conundrum*, 54 LOY. L.A. L. REV. 99 (2020).

With respect to unconscionability, see generally Uniform Commercial Code § 2-302 (2021-2022 ed.) and Restatement of the Law Second, Contracts § 208 (AM. L. INST. 1981) and cases decided thereunder.

With respect to contracts that violate public policy, see Restatement of the Law Second, Contracts §§ 178-179 (AM. L. INST. 1981) (particularly § 178(2)-(3), providing factors supporting enforcement and opposing enforcement).

With respect to contracts that have an anticompetitive effect, see Restatement of the Law Second, Contracts §§ 186-188 (AM. L. INST. 1981).

More generally, see NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019); NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS (2013); Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459 (2006).

Europe:

a. Contractual protection as compared with intellectual property protection. Rights arising out of contracts can generally be asserted only against the contractual partner. Only in a limited range of situations are they also protected against interference by third parties (see the Reporters' Notes to Principle 34). While one may assume that rights with third-party effect offer higher protection than contractual rights, this may not necessarily be the case, as rights with third-party effect do not only afford protection but may also limit party autonomy. Therefore, the absence of rights with third-party effects can be an advantage for the controller, if—based on the contractual freedom of the parties—they agreed upon a more extensive and specific protection (see Benoit Van Asbroeck, Julien Debussche and Jasmien César, Building the Data Economy – Data Ownership – Whitepaper (2017), p. 99). The *Ryanair* case from the Court of Justice of the European Union (CJEU) (Case C-30/14 ECLI:EU:C:2015:10 – *Ryanair Ltd*) is a prime example of how the absence of a right with third-party effect may lead to greater protection. In that case, the CJEU considered that the provisions on database copyright and the *sui generis* right, which limit contractual freedom, did not apply to the database in question. Consequently, the author/producer of such a database was free—subject to compliance with the applicable national law—to determine the contractual provisions governing the use of the database, which may lead to an even higher level of protection than under the provisions of the database copyright and the *sui generis* right.

b. Limits of protection between contracting parties. European legal systems usually deal with contractual restrictions on resale in the context of the acquisition of ownership. In the Germanic legal traditions, it is generally assumed that contractual restrictions do not have any third-party effect. Section 137 of the German Civil Code, for example, states that limitations on resale are void with regard to the acquisition of ownership of the second purchaser. However, the contractual promise not to resell has effect *inter partes*, and the party in breach may be liable. The German provision is quite similar to Section 364c of the Austrian Civil Code, according to which limitations on resale do not produce any third-party effect, but the validity of the agreement itself is unaffected. The French Code Civil takes a somewhat different approach. Its Article 900-1 provides that such clauses are valid under the conditions that the limitation is temporary and

justified by a serious and legitimate interest. Such a limitation of the transferability of an asset renders void any subsequent transfer within the specified period (Cass. 3e civ., 31 mai 2006, n 8 05-10270), unless the rules of good faith (Article 2276) apply.

The situation is different when it comes to copyright protected works. The resale of computer programs cannot be prohibited, because once the computer program is sold, the distribution right of that copy is exhausted, with the exception of the right to control further rental of the program or a copy thereof (Article 4(2) Directive 2009/24/EC). To what extent the exhaustion principle also applies to digital content other than computer programs is still disputed, but in a recent judgment the CJEU did not extend the first sale doctrine to e-books (Case C-263/18 ECLI:EU:C:2019:1111 –*Tom Kabinet*). In the *UsedSoft* decision, the CJEU defined "sale" as an agreement by which a person, in return for payment, transfers to another person the right to use the copy for an unlimited period (Case C-128/11 ECLI:EU:C:2012:407, para 42 ff – *UsedSoft*). The distinction between use for an unlimited period and for a limited period is thus decisive for whether a restriction on resale is effective. If the buyer is entitled to use the copy for an unlimited period of time, restrictions only have third-party effects in exceptional cases, e.g., agreements that prohibit further rental of the copyright protected work (see Article 4(2) Directive 2009/24/EC). However, if the recipient is only entitled to use the copy for a limited period of time, restrictions on resale do have third-party effect. Under the copyright law of some European Member States, the limitation on certain types of use may produce third-party effects, if the type of use is common, technically and economically independent, and thus clearly delimitable (e.g., use of a musical work for advertising purposes, German Supreme Court I ZR 226/06; see also German Supreme Court I ZR 244/97 – *OEM*).

Finally, there has been a lively discussion as to whether restrictions on use or resale can (at least) take effect against the contractual party when they are included in terms and conditions. The main argument against the validity of such agreements is that the principle of exhaustion is based on considerations of fairness. The Unfair Contract Terms Directive (UCTD) (Council Directive 93/13/EEC) considers contractual terms in consumer contracts as unfair and not binding if they are not individually negotiated and cause, contrary to the requirement of good faith, a significant imbalance between the parties' rights and obligations, to the detriment of the consumer (Article 3(1)). In several Members States, unfairness control of standard clauses is not applied only to consumer contracts but, at least in principle, extended to business-to-business (B2B) relationships. However, with regard to user accounts and computer games, the German Supreme Court decided in the famous *Half Life 2* decision that even if it is possible to resell a computer game because the right is exhausted, it is still possible to validly restrict the resale of the user account in the terms and conditions (German Supreme Court, Case I ZR 178/08 – *Half Life 2*). Nevertheless, the currently dominant view is—especially after the *UsedSoft* decision of the CJEU—that terms and conditions that are not in line with copyright law are unfair and therefore void under the UCTD. This is mainly based on the argument that the principle of exhaustion also aims to achieve a fair balance between the interests of the parties involved, just as the statutory default regimes do.

Principle 31. Unauthorized Access

(1) For the purpose of Principle 28(1)(c), access to data has been obtained by unauthorized means if it has been obtained by:

(a) circumvention of security measures;

(b) taking advantage of an obvious mistake, such as security gaps that the person accessing the data could not reasonably believe the controller had intended; or

(c) interception by technical means of nonpublic transmissions of data, including electromagnetic emissions from a medium carrying data.

(2) Access to data has not been obtained by unauthorized means if:

(a) access to the data is allowed under an agreement between the person accessing the data and the controller; or

(b) the person accessing the data had a right that, under other law (such as law relating to freedom of information and expression), prevails over the controller's right under this Principle.

Comment:

a. General observations. There are situations in which data activities do not infringe a right with third-party effect under Principle 29, or contractual limitations under Principle 30, but the activities (and, in fact, the mere access to or control of data itself) should nevertheless be considered wrongful. This is the case if a person pursuing data activities has obtained access to the data in a way that is manifestly dishonest and, among other things, disapproved by international law such as the Budapest Convention on Cybercrime.

Illustration:

137. P has raw machine data stored in password-protected cloud space provided by cloud provider C, and Y hacks the cloud space and clandestinely uses the data. Y's control is wrongful even though P does not own the medium and the data was neither protected by intellectual property law nor a trade secret. The same should apply if Y does not hack the cloud space but clandestinely intercepts the machine data during transmission to the cloud.

Apart from the situation in which a person intentionally infringes security measures or clandestinely intercepts data, the law should also intervene when a person intentionally exploits an obvious mistake by the controller. One form of such obvious mistakes is a security gap that that

person could not reasonably have believed the controller had intended. The same should hold true when access credentials have been accidentally supplied to the wrong recipient and this was obvious to the recipient.

Illustration:

138. Where, in Illustration no. 137, C's password protection scheme is down for a few hours and Y takes advantage of the situation and obtains access to P's data, this should be treated in the same manner as if Y had hacked the cloud space, because Y could not reasonably have believed that C had deliberately switched off protection.

Paragraph (1)(b) of this Principle should apply all the more if the mistake was induced by the person obtaining unauthorized access, such as by way of deceit (e.g., phishing). On the other hand, access obtained by mere noncompliance with contractual prohibitions, or with prohibitions unilaterally declared by the controller, is insufficient to make access unauthorized within the meaning of this Principle.

Illustration:

139. Z uses a webcrawler for harvesting data that happens to be publicly available in social media. In order for the webcrawler to access the social network provided by provider P, the terms and conditions need to be accepted by ticking a box, which Z (or its webcrawler) does. In P's terms and conditions, such "spidering" activities are explicitly prohibited. This might amount to a data activity that is wrongful under Principle 30, but not to unauthorized access within the meaning of this Principle.

b. Authorization. Paragraph (2) clarifies that access to or operations on data by a person are not unauthorized when authorization follows from a valid agreement between the person and the controller, or the person had a right under other law that prevails over the controller's right.

Illustration:

140. Employee E of company C terminates her employment contract with C and leaves the company, without handing over the access credentials to her workplace computer on which important company files are stored, despite a clause in the employment contract and a reminder by C. C finally gets access to the files with the help of an information technology (IT) specialist, basically hacking E's account. C has not acted in an

unauthorized manner because access to the files was authorized by the employment contract.

REPORTERS' NOTES

United States:

The U.S. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, imposes criminal and civil liability on those who knowingly or intentionally access a variety of data without authorization. The broadest category is access without authorization or exceeding authorization to information on a protected computer, defined to be computers used exclusively by financial institutions or computers used in or affecting interstate or foreign commerce or communication, including computers located outside the United States. Courts have held that evasions of internet protocol (IP) blocks and access by former employees after their authorization has been revoked constitute CFAA violations. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016); United States v. Nosal, 844 F.3d 1024, 1035-1037 (9th Cir. 2016); Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 962 (N.D. Cal. 2013). The U.S. Supreme Court is currently considering whether persons who are authorized to access information for certain purposes but access that information for an improper purpose violate the CFAA. United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), cert. granted, 140 S. Ct. 2667 (2020). Questions remain about the scope of CFAA liability for those conducting research. Compare, e.g., United States v. Auernheimer, No. 2:11-470-01, 2013 WL 1774234 (D.N.J. Mar. 19, 2013) (convicting defendant under the CFAA for program analyzing security flaw), vacated for improper venue, 748 F.3d 525 (3d Cir. 2014), with Sandvig v. Barr, 451 F. Supp. 3d 73 (D.D.C. 2020) (holding violation of terms of service insufficient to constitute a criminal violation of the CFAA).

With respect to copyrighted material, the Digital Millennium Copyright Act prohibits the circumvention of technical measures that control access to copyrighted works or manufacturing, providing, or otherwise trafficking in any technology or product capable of circumventing such technical measures. 17 U.S.C. § 1201(a)-(b).

All 50 U.S. states have enacted statutes prohibiting unauthorized access to computer systems. Computer Crime Statutes, Nat'l Conf. of State Legis. (Feb. 24, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

Europe:

a. General observations. The Budapest Convention on Cybercrime (Council of Europe Treaty No. 185, 23 November 2001) prohibits any intentional access to the whole or any part of a computer system "without right," which infringes security measures. A similar protection against the circumvention of "effective technological measures" can be found in the Information Society Service Directive (Directive 2001/29/EC). "Technological measures" is defined as any technology, device, or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter. The acquisition of a trade secret is considered unlawful under the Trade Secrets Directive (Directive (EU) 2016/943) if carried out by

unauthorized access to documents, objects, materials, substances, or electronic files that are lawfully under the control of the trade secret holder and that contain the trade secret or from which the trade secret can be deduced (Article 4(2)(a)). Similarly, the proposal for a Data Act (COM(2022) 68 final) obliges a data recipient that has abused evident gaps in the technical infrastructure of the data holder designed to protect the data to destroy the data made available by the data holder and any copies thereof (Article 11(2) Data Act proposal).

Unauthorized access to rival goods constitutes a violation of the right of possession and may be subject to possessory remedies as well as to liability claims under tort law or claims of unjust enrichment. In European legal systems, possessory remedies are usually available if interference with possession occurs without the possessor's consent or a legal ground (see Article VIII. – 6:201 Principles of European Law, Acquisition and Loss of Ownership in Good; Section 339 Austrian Civil Code; Section 858 German Civil Code).

b. Authorization. Grounds on the basis of which interference can be justified by law are, inter alia, statutory rights to withhold or rights of self-help. A person is typically entitled to withhold physical control over a good until compensated for labor or financial expenditure for the benefit of the property. The right to self-help is usually subject to very restrictive conditions. Certain jurisdictions require evidence that help by the competent state authorities would come too late (see Section 344 Austrian Civil Code). Other jurisdictions require that the self-help reaction comply with a certain standard of necessity and that it be reasonable and proportionate to the damage inflicted. Furthermore, self-help is permitted only within strict time limits. Aside from private law, interference can also be justified by public law, such as judicial enforcement proceedings.

CHAPTER B
EFFECTS OF ONWARD SUPPLY ON THE PROTECTION OF OTHERS

Principle 32. Duties of a Supplier in the Context of Onward Supply

(1) If a party supplying data to a recipient may pass the data on but is obligated to comply with duties and restrictions within the meaning of Chapter A, the law should require the supplier to:

(a) impose the same duties and restrictions on the recipient (unless the recipient is already bound by them), including the duty to do the same if the recipient supplies the data to other parties; and

(b) take reasonable and appropriate steps (including technical safeguards) to ensure that the recipient, and any parties to whom the recipient may supply the data, will comply with those restrictions.

(2) If the supplier later obtains knowledge of facts that indicate wrongful data activities within the meaning of Principle 28 on the part of a recipient, or that render data activities by the recipient wrongful or would otherwise require steps to be taken for the benefit of a protected party, the supplier must take reasonable and appropriate measures to stop wrongful activities or to take such other steps as are appropriate for the benefit of a protected party.

(3) Nothing in this Principle precludes strict vicarious liability of a controller for data activities by a processor under the applicable law.

(4) Whether the supplier's duties under this Principle may be waived by the protected party or varied by agreement to the detriment of that party is determined by the nature of the relevant duties and restrictions under Chapter A and any applicable rules of law that make those duties nonwaivable by the protected party.

Comment:

a. General observations. If data is passed on from one controller to another, it poses a challenge for the protection of others within the meaning of Chapter A. On the one hand, risks of infringement multiply with any increase in the number of controllers ultimately holding the data. The more controllers there are, the more difficult they are to identify, and it may become next to impossible for a protected party within the meaning of Chapter A to enforce its rights. On the other hand, most data existing worldwide is probably, at least potentially, subject to some restriction of

data activities following from Chapter A. Anyone receiving data from multiple sources may be confronted with a multitude of protection requirements, some of them difficult to recognize, and some of them for the remote protection of parties that are connected only through a long chain of transactions. This may have a serious chilling effect on data activities. These Principles thus need to strike a balance between third-party protection and the protection of data recipients.

Chapter B deals with the effects that onward supply of data has on the protection of other parties within the meaning of Chapter A, and the effects of such protection on the onward supply. Onward "supply" of data is to be understood broadly and is not restricted to contracts for the supply of data within the meaning of Part II, Chapter B. In particular, it includes any provision of access to the data to a processor or other service provider under Part II, Chapter C. Onward supply does not require any contract between the supplier and the recipient, in particular not when data is supplied in order to comply with an access right within the meaning of Part III. Principles 20(3) and 25(1) explicitly clarify that the duties of a supplier apply to controllers that must comply with data rights. Principles 20(2) and 24(3) ensure that data rights are afforded only with such restrictions as enable the controller to comply with both the data right and the duties under this Principle.

b. Direct effect versus due diligence duties versus strict vicarious liability. There are essentially three ways in which the law can make the difficult balance between third-party protection and the protection of data recipients.

The first possible mechanism is that of direct effect, i.e., a protected third party is afforded the same rights (and possibly remedies) against a downstream recipient as the protected third party had against the previous link in the chain of transactions. This mechanism may be part of a wider framework (see Principle 33), but it certainly cannot be the only solution, as it would both burden protected parties with enforcing their rights against a series or even a multitude of different controllers, whose identity may not even be known to them, and burden the recipients with a potential multitude of claims from parties they are not aware of.

The second possible mechanism is that of due diligence duties for suppliers, i.e., anyone who (rightfully) supplies data to another party must make sure that it chooses only recipients that will comply with the same restrictions the supplier had to comply with, and has to take further steps to safeguard the interests of protected parties, including technical and institutional safeguards. Under this mechanism, which is reflected in this Principle, the supplier is liable only for breach of its own due diligence duties, i.e., if a supplier can demonstrate that it has done everything that

could be expected from it, and, despite all safeguards, a downstream supplier engages in wrongful data activities, the supplier would not be liable to a protected third party for the activities of the downstream recipient.

The third possible mechanism is that of strict vicarious liability. Under this mechanism, the law remains largely silent as to the duties of a supplier when passing on data, but whoever passes on data does so at its own risk and will be strictly liable for whatever happens in terms of wrongful data activities downstream. On the one hand, this is efficient, as it leaves the decision as to the appropriate safeguards to the supplier and lowers overall costs of compliance. On the other hand, liability risks may become incalculable if the recipient again passes the data on, assuming that the first supplier is also liable for any wrongful activities far down the chain of transactions (if a law opted for this model but failed to provide for liability of the supplier for activities further down the chain of transactions this might lead to massive undercompensation of protected parties suffering harm). Also, the supplier is not always the stronger party, but may be a small retailer passing data on to a multinational company and without much of a choice, which would make it seem inequitable to hold that retailer strictly liable for anything wrongful happening downstream. This is why, ultimately, these Principles do not propose strict vicarious liability as the general rule. However, strict vicarious liability may be justified if data is entrusted to a service provider within the meaning of Part II, Chapter C; see paragraph (3).

c. Duty to pass on restrictions. Paragraph (1)(a) of this Principle provides in the first place that, even when onward supply of data as such is rightful, the supplier of data is under a duty to pass on to the recipient all the duties and restrictions that the supplier itself had to comply with for the benefit of a protected party within the meaning of Chapter A, unless the recipient is already bound by those duties and restrictions. This includes the duty to impose the same duties and restrictions on any downstream recipient to which the recipient may, in turn, make the data available. In most cases, protected parties will be either holders of intellectual property rights with regard to the data or data subjects protected under data privacy/data protection law (i.e., parties protected under Principle 29) or upstream suppliers that had imposed on the supplier particular contractual limitations under Principle 30. In some cases, such as when protected parties are holders of intellectual property rights, recipients would likely be already bound by the restrictions imposed by the intellectual property regime in any case.

When the duty or restriction already follows from the law, all that is normally required by paragraph (1)(a) of this Principle, without prejudice to more far-reaching duties under paragraph

(1)(b), is that the supplier choose trustworthy recipients, i.e., apply due diligence in assessing whether the recipient will most likely act in a compliant manner, and, when necessary, inform those recipients of the existence of the relevant rights on the part of protected parties. However, when the duty or restriction would normally bind only the supplier, such as a contractual duty or restriction, the supplier may not supply the data to a recipient that does not agree to comply with the same duties or restrictions. If the supplier still passes that data on, this data activity would be considered wrongful under these Principles and, if the requirements of Principle 34 are met, also the data activities of the recipient.

Illustration:

141. Supplier S of bulk data agrees with the first recipient R1 that R1 may use the data for all lawful purposes except a defined list of purposes that would harm S's economic interests. If R1 supplies the data to R2 (provided this is not excluded under the contract with S), R1 is under an obligation to impose the same restrictions with regard to data use on R2, i.e., under the contract with R1, R2 also must agree not to process the data for the defined list of purposes that would harm S's economic interests.

In particular when due diligence leads to the assessment that the recipient might not effectively comply with the duties and restrictions imposed, the supplier must, under paragraph (1)(b) of this Principle, adopt additional safeguards that provide an appropriate level of certainty, or refrain from making the data available to the recipient. Such additional safeguards can be of a legal nature, such as prohibitively high penalties (when allowed) in cases of noncompliant activities, or of a technical nature, such as technical means that ensure that noncompliant activities are prevented. They may also include institutional arrangements such as using the services of a data trustee or data escrowee within the meaning of Principles 13 and 14.

These Principles do not define exactly which steps can be expected in which kind of situation. Generally speaking, a risk-based approach must be taken, i.e., the more "sensitive" the data and the greater the potential risks for protected third parties that may follow from noncompliant data activities, the stricter and more effective the safeguards the supplier must ultimately take. The steps that can reasonably be expected from a supplier also depend on the relationship between the supplier and the recipient. If the recipient is a processor that processes the data on the supplier's behalf, the supplier normally has greater influence on the recipient and on

how the recipient deals with the data (but this is not necessarily the case, e.g., when a small business uses the services of a big processor, such as a big cloud space provider).

d. Duty to monitor and remediate wrongful activities. Paragraph (2) stresses that, when the supplier later obtains knowledge of facts that indicate wrongful processing on the part of the recipient, render data activities by the recipient wrongful, or would otherwise require steps to be taken for the benefit of a protected party, the supplier must take reasonable and appropriate steps to stop wrongful activities, and protect the protected party. The reason why paragraph (2) requires knowledge (and not merely "notice") is that a controller can normally not be expected to continuously monitor and call into question any kind of onward supply that occurred in the past. This normally means that the supplier must inform the recipient when the recipient may be unaware of the wrongfulness. The technical and other arrangements must be such as to ensure that the information reaches the recipient as early as the circumstances require, in particular when the recipient is a processor.

Illustration:

142. Business S operates a video game and supplies personal user data to recipient R, which is lawful under the applicable European data protection regime because users have given consent. When S learns of the withdrawal of consent by some of its users, further control by both S and R of this personal user data will usually become wrongful, and they will usually be under an obligation to erase this data. S must pass this information on to R in order to direct R to erase the data. If R is not a controller, but a processor processing data on behalf of S, S must take even more rigorous action and immediately stop processing by R of the data of the users who have withdrawn consent.

However, paragraph (2) of this Principle only requires steps that are reasonable and appropriate, again taking a risk-based approach and considering the relationship between the supplier and the recipient, including the degree of influence that the supplier has on the recipient.

Illustration:

143. W runs a website with a large quantity of information that can be downloaded freely. W then learns that one of the documents offered for download infringes X's copyright, and therefore W immediately takes it off the website. W is aware that the document has been downloaded 300 times, but W has no reasonable means of finding out

who those individuals are and how to contact them. In this situation, there is no obligation to inform those individuals or take further action under this Principle.

e. Waiver of duties. Whether the supplier's duties under this Principle may be waived by the protected (third) party or varied by agreement to the detriment of that party is determined by the nature of the relevant duties and restrictions under Chapter A. If, for instance, the restriction stems from a mandatory statutory regime such as data privacy/data protection law, any waiver by the protected party, if it is at all possible, must occur within the boundaries set by that statutory regime, which will be rather narrow. If the restriction stems from a contract between the protected party and the supplier, the protected party can waive protection within the much broader limits set by the applicable contract law, which may differ from jurisdiction to jurisdiction, and from scenario to scenario (e.g., depending on whether the transaction is a business-to-consumer or business-to-business transaction).

REPORTERS' NOTES

United States:

Contractual provisions embodying the duty to pass on restrictions are quite common in the United States. See, for example, the following language:

> Each sublicense granted by a Party to a Third Party pursuant to Sections 2.1(b) or 2.2(b) (a "Sublicense") shall (a) be in writing; (b) be subject and subordinate to, and consistent with, the terms and conditions of this Agreement; and (c) require the applicable sublicensee (the "Sublicensee") to comply with all applicable terms of this Agreement.

Law Insider, Sublicense Requirements Sample Clauses, https://www.lawinsider.com/clause/sublicense-requirements (emphasis added). Similarly, it is quite common for data license contracts to impose on a licensee a duty to monitor the compliance with license terms by the sublicensee. See Daniel Glazer et al., Data as IP and Data License Agreements, Westlaw Practical Law Practice Note 4-532-4243, available at https://www.friedfrank.com/siteFiles/Publications/Data%20as%20IP%20and%20Data%20License%20Agreements%20(1).pdf (a sublicense agreement should expressly specify "appropriate sublicensing obligations (for example, the sublicensor's responsibility for the actions of its sublicensees . . . ")).

Some federal statutes require suppliers of data to impose legal duties on recipients. For example, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires covered entities wishing to disclose protected health information to "business associates" to obtain satisfactory assurances that the business associates will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and

will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Europe:

c. Duty to pass on restrictions. Duties to pass on restrictions can be found in the Standard Contractual Clauses (SCC) for the transfer of personal data between European Union (EU)/European Economic Area (EEA) and non-EU/EEA countries (Commission Implementing Decision (EU) 2021/914). If an exporting controller and an importing controller or processor include the SCC in their contract, the transfer of the data outside the EU/EEA is considered to be in accordance with EU data protection legislation. However, according to a recent judgment of the Court of Justice of the European Union (CJEU) (C-311/18 ECLI:EU:C:2020:559 – *Schrems II*), further steps may be required, such as establishment of a data escrow. Similar to Principle 33, the terms of SCC differ depending on whether the importing recipient is a controller or processor.

The purpose of SCC is to ensure compliance with the requirements of the General Data Protection Regulation (GDPR) (Clause 1(a)). The exporter, i.e., the supplier, warrants, that it has used reasonable efforts to determine that the data importer, i.e., the recipient, is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses (Clause 8). If the importer is unable to comply with the SCC for whatever reason, it shall promptly inform the data exporter (Clause 16(a)). The exporter shall be entitled to terminate the contract, e.g., if the importer is in substantial breach or persistent breach of the SCC.

If the importer is a controller, the SCC provide for several obligations on data protection safeguards. The importer shall, inter alia, not disclose the data to a third party located outside the EU unless the third party is or agrees to be bound by the SCC. Moreover, the importer shall deal with any enquiries and requests it receives from a data subject relating to the processing of his or her personal data and the exercise of his or her rights under the SCC without undue delay and at least within one month of the receipt of the enquiry.

Different rules in the SCC apply if the entity to whom the data is transferred is a processor established outside the EEA. The fact that the importer processes the data on behalf of the controller (exporter) justifies the enhanced obligations of the supplier to monitor the compliance of the processor (cf. paragraph (1)(b) of this Principle). While the exporter also warrants that it has used reasonable efforts to determine that the importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under the SCC, the importer shall process the personal data only on documented instructions from the data exporter (Clause 8 Module Two 8.1(a)). They may give such instructions on the processing of the personal data throughout the duration of the contract. The SCC also contain rules on the use of sub-processors. Pursuant to Clause 9, the importer may only subcontract any of its processing activities with written authorization from the exporter. If the authorization has been obtained, the importer shall impose the same obligations on the sub-processor as are imposed on the data importer.

A duty to pass on restrictions can also be found in the GDPR (Regulation (EU) 2016/679) for the sub-processing of personal data. According to Article 28(4), when a processor engages another processor to carry out specific processing activities on behalf of the controller, the processor must impose on the sub-processor the same data protection obligations as set out in the

contract or other legal act between the controller and the initial processor, either by way of contract with the sub-processor or other legal act under EU or Member State law. Those obligations are, inter alia, that the processor must process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization (Article 28(3)(a)). Furthermore, the processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28, and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Article 28(3)(h)). However, other than the SCC, the GDPR does not specifically address the onward transfer from one controller to another. Articles 28 and 29 contain a series of specific provisions only for controller-to-processor transfers; controller-to-controller transfers are only indirectly covered by the general provisions on data processing. Given that the existence of controller-to-controller transfers cannot have escaped the attention of the European legislator, it will be difficult to apply the detailed requirements that Articles 28 and 29 of the GDPR have established for controller-to-processor transfers simply by analogy (see Christiane Wendehorst, Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?, in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmeyer (eds.), Data as Counter-Performance – Contract Law 2.0?, 2020, p. 191, 217 ff.).

A slightly different approach was taken in the Data Governance Act (DGA) (Regulation (EU) 2022/868), which sets out conditions for the re-use of protected data held by the public sector. The DGA does not put forward an explicit obligation that a re-user, who intends to transfer public sector data that is confidential or protected by intellectual property rights to a third country, must pass on any restrictions to the recipient. However, Article 5(10) stipulates that the public sector body shall only transmit protected data to a re-user who intends to transfer the data to a third country if the re-user undertakes to comply with the obligations imposed by intellectual property law or confidentiality agreements even after the data is transferred to a third country. Furthermore, the re-user also needs to accept the jurisdiction of the courts of the Member State of the public sector body regarding any dispute related to compliance with that obligation. This rule does not apply if the re-user transfers the data to a third country that has been declared to provide similar protection of trade secrets and intellectual property (Article 5(12)). In essence, Article 5(19) establishes strict liability of the re-user of public data for any violations of trade secret or intellectual property protection by a downstream recipient that is located in a non-EEA country. While re-users of publicly held data are not explicitly required to pass on restrictions, they will likely do so in order to reduce the risk of being exposed to liability claims. The DGA deviates from Principle 33 because under this Principle, the supplier would not be liable for any breaches of a recipient if the supplier passed on its duties and restrictions to the recipient and took reasonable and appropriate steps to ensure compliance with these restrictions.

d. Duty to monitor and remediate wrongful activities. A duty to inform the recipient of the transferred data that is similar to the one stated in paragraph (2) of this Principle can be found in the GDPR (Regulation (EU) 2016/679). According to Articles 16 to 18, data subjects have the right to request the rectification, erasure, and restriction of further processing of their personal data. The controller that receives such a request is, pursuant to Article 19, under an obligation to communicate the request to each recipient to whom the personal data has been disclosed. A

controller is exempted from this obligation if such communication proves impossible or involves disproportionate effort (cf. paragraph (2) of this Principle). Furthermore, Article 17(2) obligates controllers that have made personal data public to take reasonable steps, taking account of available technology and the cost of implementation, to inform controllers that are processing the personal data that the data subject has requested the erasure by such controllers. Once the information reaches the recipient, that recipient is not automatically obligated to comply with the request, as the processing may still be justified by a separate legal ground. (see Christiane Wendehorst, Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?, in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmeyer (eds.), Data as Counter-Performance – Contract Law 2.0?, 2020, p. 191, 209 ff.).

Principle 33. Direct Action against Downstream Recipient

When an immediate recipient of data has a duty under Principle 32 vis-à-vis its supplier to impose particular terms on a downstream recipient to whom the immediate recipient will supply the data, and when the immediate recipient has complied with that duty but the downstream recipient breaches the terms imposed on it, the initial supplier may proceed directly against the downstream recipient after giving notice to the immediate recipient.

Comment:

a. Direct action. When data is passed on by the immediate recipient, two relationships result: one between the initial supplier and its recipient and one between that recipient, now acting as a supplier, and the downstream recipient. It is useful to distinguish between those two relationships in which noncompliance may occur. If the immediate recipient passes the data on to the downstream recipient in breach of terms imposed on it under Principle 32, the immediate recipient is accountable for the wrongful data activities, without prejudice to any additional accountability of the downstream recipient under Principle 34.

Illustration:

144. Assume that business Y in Illustration no. 134 has concluded a valid contract with airline X that defines, inter alia, the conditions under which Y may pass the data harvested from X's website on to third parties. These conditions provide that Y may transfer the data only to third parties within its own group of companies, and that when Y does so, Y is under a duty to impose the same condition on the third party. When Y, in breach of the contract with X, transfers the data to agency Z outside Y's group of companies, this is an

issue between the immediate contracting parties X and Y. Z is not liable unless its conduct—such as a failure to act in good faith—creates a separate ground of liability.

When, on the other hand, the immediate recipient fulfills all its duties under Principle 32 and imposes the restrictions on the downstream recipient plus takes all other steps that may be required in the circumstances, but then, unforeseeably, the downstream recipient is noncompliant, the immediate recipient has done all that could be expected from it. Subject to any strict vicarious liability under Principle 32(3), the supplier is not liable, but this Principle allows the initial supplier to enforce directly against the downstream recipient.

Illustration:

145. When, in a scenario such as the one described in Illustration no. 144, agency Z does belong to Y's group of companies and the contract between Y and Z does impose on Z the duty to refrain from passing the data on to fourth parties outside the group of companies, but when Z then breaches this duty owed to Y, this is a case for this Principle. In this case, X would have direct remedies against Z.

In many jurisdictions, taking direct enforcement action against the downstream recipient is already possible under a range of doctrines, such as concepts of implied assignment (of claims the immediate recipient has against the third party), constructive trust, subrogation to a claim for damages, or, when available, treatment of the supplier as a third-party beneficiary of its immediate recipient's contract with the downstream recipient. This Principle advises that the law should seek to achieve this result. The requirement that the initial supplier first give notice to the immediate recipient may be seen as similar to notice requirements in some types of derivative law suits. Unlike derivative law suits, however, any recovery awarded in such a direct action is normally for the benefit of the initial supplier.

This Principle does not address defenses that the downstream recipient would be able to raise against its immediate supplier. Normally, the downstream recipient may also raise such defenses against the upstream supplier. However, there may be some doctrines external to these Principles that bring about a different result in some cases.

REPORTERS' NOTES

United States:

For U.S. law regarding third-party beneficiaries, see generally Restatement of the Law Second, Contracts §§ 302-315 (AM. L. INST. 1981).

A third party may recover for the breach of a contractual promise if both parties intended to recognize a right to performance in the third party and either the performance of the promise will satisfy an obligation of the promisee to the beneficiary or the promisee intended to give the benefit of said performance to that third party. Restatement of the Law Second, Contracts § 302 (AM. L. INST. 1981). In the absence of such intent, some states will not allow recovery by third-party beneficiaries. See, e.g., Katz v. Pershing, LLC, 672 F.3d 64, 73-74 (1st Cir. 2012). Contractual provisions reserving enforcement to other parties may bar even expressly intended beneficiaries from bringing suit. See, e.g., In re TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83, 88-90 (D. Mass. 2007). When manifestations of intent are unclear, overriding social policies, which may be embodied in statutes, may require giving third parties the right to enforce contractual rights without regard to the intention of the parties. Restatement of the Law Second, Contracts, Chapter 14, Introductory Note, and § 302, Comment *d* (AM. L. INST. 1981).

In the absence of an express non-assignment provision, contractual rights may generally be assigned to third parties unless such assignment would violate statute or public policy, materially change the obligor's duty, or have a materially detrimental effect on the obligor's expectations (such as by increasing the burden imposed upon him or her or reducing his or her value received). Restatement of the Law Second, Contracts § 317(2) (AM. L. INST. 1981); Uniform Commercial Code § 2-210(2) (2021-2022 ed.). Equity may also permit third-party enforcement by construing contracts making downstream transfers of an asset to include an implied assignment of restrictions contained in the contract effecting the initial transfer. Charles I. Giddings, *Restriction Upon the Use of Land*, 5 HARV. L. REV. 274, 284 (1892).

Courts may also use their equitable powers to treat a party that is unjustly enriched by its wrongful acquisition of an asset as holding that asset in constructive trust for the equitable owner of the asset, particularly when the asset has special value for the claimant, when it has appreciated, or when its value is difficult to establish. Restatement of the Law Third, Restitution and Unjust Enrichment § 55(1) and Comment *c* (AM. L. INST. 2011).

Europe:

Direct actions vis-à-vis a downstream party within a contractual value chain can be achieved by assigning the immediate recipient's claims against the downstream recipient to the supplier. In general, European contract law allows not only the assignment of present claims but also of future claims that arise out of an existing contractual relationship. However, there are some restrictions, for example, when the assignment would be against public policy or when the rights are personal to the creditor (see Hein Kötz, European Contract law, 2nd Edition, 2017, pp. 342 ff.). The assignment of claims usually transfers the rights to performance in respect of the claim assigned as well as all accessory rights securing such performance, and would thus also cover

remedies in cases of non-performance (see Chapter 11 Principles of European Contract Law (PECL); Article III. – 5:101 ff Draft Common Frame of Reference (DCFR)).

Another possibility that would lead to a direct action by the supplier against the downstream recipient under this Principle is to conclude a contract in favor of a third party, i.e., the immediate recipient and the downstream recipient agree that the supplier may require performance against the downstream recipient (cf. Article 6:110 PECL; Article II. – 9:301 DCFR). Under such a contract, the third party, i.e., the supplier, has the same rights to performance and remedies for non-performance as if the downstream recipient were bound to render the performance under a binding, unilateral undertaking in favor of the supplier (Article II. – 9:302 DCFR). However, the downstream recipient may assert against the supplier all defenses that the downstream recipient could assert against the immediate recipient. For a long time, it was disputed whether contracts in favor of a third party would need the consent of the third party or not. Under most European jurisdictions, consent of the third party is not required, but the third party may reject the right or benefit (see Article II. – 9:303 Draft Common Frame of Reference (DCFR); Section 881 Austrian Civil Code; Section 333 German Civil Code or Section 1411(3) French Code Civil; see also Section 1 of the Right of Third Party Act 1999 in the United Kingdom).

Under French law, direct actions in contractual value chains can be taken by means of the *action directe* in so-called *chaînes de ventes* (sales chains). The *action directe* is based on an early judgment of the Cour de Cassation in which the court ruled that a warranty attached to a contract of sale could pass on to the next buyer when the item was resold (Cass. civ., 25 January 1820, S. 1820, 1, 171). Thus, if A sells a good to B, and B sells that good to C, C could rely on the warranty attached to the first contract and bring a claim for breach of a contractual warranty against A. The legal nature of the *action directe* is still disputed. While some authors argue that the warranty claims are transferred along with the thing that is being sold as an accessory (see Jean-Sébastien Borghetti, Breach of Contract and Liability to Third Parties in French Law: How to Break the Deadlock?, 2010 *Zeitschrift für Europäisches Privatrecht*, p. 279, 285 ff), others argue that the claims are (tacitly) assigned (see Hein Kötz, European Contract law, 2nd Edition, 2017, 329 ff.). The main difference between the French *action directe* and the direct action under this Principle is that the two actions are enforced in opposite directions along the contractual chain. Under the *action directe*, the last buyer of a good can act directly against the initial seller (up the contractual chain), while under this Principle the initial supplier of data can act against any downstream recipient (down the contractual chain).

Direct contractual actions under this Principle should not be confused with so-called vicarious liability, under which agents are liable for the actions of their auxiliaries (see Art 6:102 Principles of European Tort Law). Such vicarious liability can also be found in Article 28(4) of the General Data Protection Regulation (GDPR) with regard to sub-processing contracts. If the sub-processor fails to fulfill its data protection obligations, the initial processor remains fully liable to the controller for the performance of the other processor's obligations.

Principle 34. Wrongfulness Taking Effect vis-à-vis Downstream Recipient

(1) In addition to wrongfulness following directly from Chapter A, a data activity by a downstream recipient that has received the data from a supplier is wrongful when (i) control by that supplier was wrongful, (ii) that supplier acted wrongfully in passing the data on, or (iii) that supplier acted wrongfully in failing to impose a duty or restriction on the downstream recipient under Principle 32 that would have excluded the data activity, and the downstream recipient either:

(a) has notice of the wrongfulness on the part of the supplier at the time when the data activity is conducted; or

(b) failed to make such investigation when the data was received as could reasonably be expected under the circumstances.

(2) Paragraph (1) does not apply when:

(a) wrongfulness on the part of the supplier was not material in the circumstances and could not reasonably be expected to cause material harm to a party protected under Chapter A;

(b) the downstream recipient obtained notice only at a time after the data was supplied, and the downstream recipient's reliance interests clearly outweigh, in the circumstances, the legitimate interests of a party protected under Chapter A; or

(c) the data was generally accessible to persons that normally deal with the kind of information in question.

(3) Paragraphs (1) and (2) apply, with appropriate adjustments, to data activities by a party that has not received the data from a supplier but that has otherwise obtained access to the data through another party.

Comment:

a. General observations. This Principle deals with the situation when data is supplied to a downstream recipient and when there is a protected third party within the meaning of Chapter A, but when the rights interfered with do not directly take effect vis-à-vis the downstream recipient. This could be the case, for example, when an upstream supplier makes data available to an immediate recipient only under contractual limitations within the meaning of Principle 30 and the immediate recipient then wrongfully passes the data on to a downstream recipient without those restrictions; or when a party's data is accessed by unauthorized means within the meaning of

Principle 31 and the "data thief" then sells the data to a downstream recipient. In all these cases, the immediate recipient or thief would of course be acting wrongfully, but this Principle defines the conditions under which data activities by the downstream recipient are also wrongful.

Under many legal systems, a third party could become liable vis-à-vis a protected party (such as an upstream supplier) if the third party has or gains knowledge of the fact that the data was obtained through a breach of contract. Liability of the third party would usually be in tort, such as under tortious interference and equivalent concepts. The rationale would normally be that the third party, directly or indirectly, instigated the second party to breach its obligations vis-à-vis the first party or otherwise took part in the wrong committed by the second party vis-à-vis the first party. Such third-party liability may be "weak" (e.g., there is liability only when the third-party had positive knowledge of the wrong, and only when knowledge was present at the time of the initial acquisition) or "strong" (e.g., there is also liability when the third party was acting negligently, and also when the third party continued the activities after learning the truth at a point in time after the initial acquisition).

This Principle is essentially of tort-law logic and has opted for a rather "strong" form of third-party liability, which goes beyond what we find in most legal systems, in the context of interference with contract in general, but remains clearly below what we usually find in the context of interference with tangible property. The solution suggested is similar to a solution that is not uncommon in trade secrets law. This is a policy choice made by these Principles, which seek to strike a balance between the legitimate interests of downstream recipients and those of any protected parties.

This Principle is without prejudice to Chapter A, i.e., if a data activity by a downstream recipient is already wrongful because the downstream recipient was acting in violation of its own contractual duties, or was itself violating applicable standards of data privacy/data protection law, this is and remains wrongful under Chapter A.

b. Conditions for wrongfulness. According to paragraph (1), data activities by a downstream recipient may be wrongful even when there is no direct wrongfulness under Chapter A on the part of the downstream recipient itself, but when such wrongfulness was present on the part of the supplier from whom the downstream recipient received the data and either the downstream recipient has notice of the wrongfulness on the part of the supplier at the time when the downstream recipient conducts the relevant data activity or the downstream recipient failed to make such

investigation, at the time when the data was received, that could reasonably be expected under the circumstances.

This could be the case in situations in which control by the supplier was wrongful as such, i.e., when the supplier should not have gained or retained control of the data at all.

Illustration:

146. Start-up company S is developing a new robot. For "training" the robot's intelligent software, S would need huge amounts of industry data that the controllers of the data are either not prepared to make available to S or are offering at a price S cannot afford. Fortuitously, S is offered suitable data at an affordable price from backstreet business B, and without asking questions about how B got the data, S makes the deal and uses the data for training the robot. If B gained control of the data by hacking other people's servers, S was not rightfully in control of the data, because S failed to make the investigations that could reasonably be expected under the circumstances when buying the data.

Even if the supplier was rightfully in control of the data, the supplier may not have been allowed to pass the data on to the downstream recipient, for example, because of a contractual limitation under Principle 30. Even if the supplier was allowed to pass the data on to the downstream recipient, the supplier may have been under an obligation to impose restrictions on the downstream recipient under Principle 32 and may have failed to do so. In all these cases, the supplier would have been acting wrongfully, but, if it were not for this Principle, this would not mean that wrongfulness on the part of the supplier affects data activities by the downstream recipient.

Illustration:

147. Assume that B in Illustration no. 146 did not hack other people's servers, but was a data trustee within the meaning of Principle 13 who promised to the entrusters not to make the data available to third parties within a defined range of industries (including the industry to which S belongs) because that might harm the economic interests of the entrusters. If S had (or later gains) notice of this restriction or failed to make the investigations that could reasonably be expected under the circumstances at the time the deal with B was made, and nevertheless continues its data activities, S is acting wrongfully.

The level of care that can be expected from a downstream recipient is higher at the point in time when the downstream recipient acquires the data, at which time the downstream recipient must take reasonable and appropriate steps to ascertain whether the supplier was acting rightfully. These Principles do not define the precise steps required in each kind of scenario. Generally speaking, a risk-based approach should also be applied in this context. So, for example, the sort of investigation called for by paragraph (1)(b) increases in importance as risks increase. More specifically, the less information the downstream recipient has about the supplier and the original data sources, the fewer indications there are that the supplier is trustworthy, the higher the probability that there are restrictions within the meaning of Chapter A and the higher the potential risk for protected parties, the more inquiries a downstream recipient can be expected to make.

Illustration:

148. In Illustration no. 146, a court would consider that S was well aware that the "regular" controllers of the data are normally unwilling to make them available, so if B suddenly is in control of such data, in particular as a "backstreet" type of business, that is reason for S to be on alert. In such a situation, S should make thorough inquiries. If, on the other hand, S makes a deal directly with company C whose machines generate the industry data, the probability that another party has a better right to the data than C is rather low, as is the burden on S to make further inquiries.

Even if the downstream recipient made the investigations that could reasonably be expected under the circumstances at the time when the acquisition was made, actual notice obtained at a point in time after the data acquired may still render data activities wrongful, but only for the future. The downstream recipient that obtains notice must stop the relevant data activities.

c. Protection for downstream recipients. The rule in paragraph (1) is potentially far-reaching and may entail high risks for downstream recipients. This is why the rule needs to be restricted in a number of cases, which are listed in paragraph (2).

The rationale of paragraph (2)(a) is that of a de minimis rule. With data, a multitude of restrictions could follow from all sorts of directions, including, in particular, very detailed data privacy or data protection regulation and a host of far-reaching restrictions imposed by contractual means as a matter of routine in standard contract terms. Those restrictions could accumulate, with the possibility that the data would also be "tainted" for onward recipients. If onward transferees are subject to all such accumulated restrictions, it could add significant risk to the data economy

because there would be no "untainted" data. Accordingly, some sort of rule protecting transferees is necessary in order to avoid over-deterring data transfers. Despite notice of wrongfulness on the part of the supplier, a downstream recipient should still not act wrongfully if the wrongfulness on the part of the supplier (of which the recipient has notice) is not material and could not reasonably be expected to cause material harm to protected third parties.

Illustrations:

149. Real property business R hires company D to create digital twins of R's buildings to facilitate maintenance. The data is to be transferred to R in order to enable R to respond where repair is needed. D clandestinely sells some of this data to local tourist guide organization T because some of the photos include a view of the beach at sunset. This may be in breach of the contract D has with R, as D may not be allowed under this contract to pass data on to third parties, but under the given circumstances, this breach is not material and cannot really cause harm to R (assuming that making the deal with T himself would never have crossed R's mind, R does not lose a business opportunity, and R does not have copyright in the material). So, T would be allowed to keep the photos even if T had been aware of how D obtained the photos (but any liability on the part of D would remain unaffected).

150. If D in Illustration no. 149 instead sells the photos to X, who runs a database that seeks to warn potential buyers of immovable property against buying premises that are in bad shape, this may harm R's interests, so notice on the part of X that D acted wrongfully clearly makes control by X wrongful.

Generally speaking, a case-by-case assessment needs to be made to decide whether or not a violation or breach on the part of the supplier is material. In doing so, one must take into account, in particular, the significance of the duty breached for the legitimate interests of the protected party and whether the supplier was acting purposely, recklessly, negligently, or innocently. As far as contractual restrictions within the meaning of Principle 30 are concerned, cautious analogies could be drawn to doctrines relating to material breach of contract. Unauthorized access within the meaning of Principle 31 would usually be considered to be material, but there may be exceptions; for example, when security measures taken were very weak and it would not be justified to assume downstream third-party effects. In assessing potential harm to the protected party, an objective standard seems appropriate.

Illustration:

151. In Illustration no. 149, if R subjectively feels uneasy about one of his buildings being visible on a photo used by a tourist guide company, that would not be sufficient to make control by T wrongful. Control by T would be wrongful even without any objective risk of harm only if, in the contract between R and D, this had been specifically highlighted as important, thus making the breach by D a material breach.

Paragraph (2)(b) is an exception from paragraph (1) for downstream recipients who exercised due diligence when acquiring the data and who have taken further steps and made further investment in reliance on the acquisition of the data. While the downstream recipient's reliance cannot generally outweigh the legitimate interests of the protected third party, there may be situations in which, on balance, the downstream recipient's interests should take priority.

Illustration:

152. R acquires large amounts of data required for training a new artificial intelligence (AI) from S at a price of several million U.S. dollars. When making the deal with S, R diligently checks the relevant documents made available to it and makes all enquiries that can reasonably be expected about the origin of the data, and S provides representations and warranties that it has the legal right to sell the data. In reliance on the availability of the data, R invests another several million U.S. dollars in the development of the AI. Three years later, it becomes apparent that, for reasons R could not reasonably have detected, S was actually not allowed to sell the data to R because of an unexpected third-party claim from S's parent company P. A court should take into account the huge economic harm R would suffer if it must stop using the data, that R had been acting diligently, and that P should have monitored the activities of its subsidiaries to make sure its rights were not infringed. A court might thus conclude that R's legitimate interests outweigh those of P and S, and that R may continue using the data.

Finally, a downstream recipient's data activities should not be considered wrongful when the information was generally accessible to persons within circles that normally deal with the kind of information in question.

Illustration:

153. Through unauthorized access to C's servers, S obtains a number of chemical formulas associated with patents held by C and sells the data to R. The chemical formulas are available to any interested party from the patent office, and have subsequently been published in scientific journals. Processing of the chemical formulas by R should not be considered wrongful even if R was aware of how S had obtained access to the data, because R could, at any time, have made the effort to obtain the data from the patent office or from scientific journals.

d. Application to similar situations. There are some situations in which the conditions of paragraph (1) are not strictly fulfilled because there was no supply, but it would still be appropriate to apply the same rules. This is why paragraph (3) provides that paragraphs (1) and (2) apply with appropriate adjustments to data activities by a party that did not receive the data from a supplier but obtained access to the data through another party.

Illustration:

154. Parent company P supplied data to subsidiary S, explicitly prohibiting any onward transfer to third parties without the explicit consent of P. After R has not succeeded in persuading S to sell R the data, R hacks S's servers and obtains unauthorized access to the data. S then becomes insolvent and is no longer able to take action against R, or no longer interested in doing so. However, while the data has not been "supplied" to R by S, data activities by R are not only wrongful vis-à-vis S, but also vis-à-vis P.

REPORTERS' NOTES

United States:

Current law on tortious interference with contract incorporates what Comment *a* calls "weak" third-party liability, which requires intent. Restatement of the Law Third, Torts: Liability for Economic Harm §§ 7(b), 17(1)(d)-(e) (AM. L. INST. 2020). Courts have required intentional conduct when evaluating claims of tortious interference with rights to data. See 3D Glob. Sols., Inc. v. MVM, Inc., 552 F. Supp. 2d 1, 9-10 (D.D.C. 2008). Other courts have similarly refused to allow claims based on mere negligence for data security breaches that caused purely economic losses. See In re TJX Cos. Retail Sec. Breach Litigation, 524 F. Supp. 2d 83, 90-91 (D. Mass. 2007). The law of restitution may also permit recovery of gains obtained by a party that interfered with business relations. Restatement of the Law Third, Restitution and Unjust Enrichment § 44 (AM. L. INST. 2011). Equitable remedies, such as constructive trusts, are not available for the

conduct of bona fide purchasers prior to their receiving notice of the potential wrongfulness of their possession of the asset in question. Restatement of the Law Third, Restitution and Unjust Enrichment § 66 (AM. L. INST. 2011).

As Comment *a* notes, the endorsement of "strong" third-party liability represents a policy choice largely derived from trade secret law, which imposes liability for uses or disclosures of trade secrets that actors know or have reason to know were wrongfully obtained. Restatement of the Law Third, Unfair Competition § 40(b) (AM. L. INST. 1995); Uniform Trade Secrets Act (UTSA) § 1(2)(ii)(B)(III) (1985). Trade secret law does not provide immunity for onward transferees that obtain knowledge of wrongfulness after the time of transfer, although it bases the determination of monetary relief on factors such as the fact and extent of pecuniary losses and gains, the nature and extent of the appropriation, and good-faith reliance, among other things. Restatement of the Law Third, Unfair Competition § 45(2) (AM. L. INST. 1995); UTSA § 3, Comment. In addition, trade secret law may not require defendants to relinquish all profits when they have made good-faith investments in the trade secret prior to receiving notice of the plaintiff's claim. Restatement of the Law Third, Unfair Competition § 45, Comment *g* (AM. L. INST. 1995); UTSA § 3(a). Injunctive relief similarly depends on the nature of the interest and the appropriation, the likely harm, and good faith, among other factors. Restatement of the Law Third, Unfair Competition § 44(2) (AM. L. INST. 1995); UTSA § 2, Comment. Unqualified injunctive relief may not be appropriate when good-faith defendants have made substantial investments in reliance on the trade secret prior to notice that it had been misappropriated. Restatement of the Law Third, Unfair Competition § 43, Comments *b* and *c* (AM. L. INST. 1995); UTSA § 2(b). This approach rejects the one taken in Restatement of the Law, Torts § 758(b) (AM. L. INST. 1939), which accorded absolute immunity to good-faith transferees.

Europe:

As contractual rights are relative in nature, they can only be infringed by persons who owe a corresponding obligation to the holder of the right. An exception to this fundamental principle is the inducement of non-performance of a contractual obligation, which gives rise to non-contractual liability under all European jurisdictions and previously existed in Roman law. The underlying rationale is that when a third party intentionally induces a person not to perform contractual or other obligations to another party, that party who thereby suffers loss may claim reparation from the person inducing the non-performance (see Article 2:211 Principles of European Law – Non-Contractual Liability Arising out of Damage Caused to Another; Article 2:211 Draft Common Frame of Reference (DCFR)). In some European legal systems, liability not only arises when a person intentionally induces the infringement of an obligation, but also when that person knows or should have known of the breach of the obligation.

For example, under French law, a tortious *faute* is committed if a person knowingly aids another person in breaching a contractual obligation. Liability arises vis-à-vis the party who is affected by this breach of contract, and it suffices that the person inducing the breach had knowledge of the existence of the contract (Cass.civ. 17, Bull.civ. 2000, I, no. 246 p. 161). In Austria, it is undisputed that inducing a breach of contract with the intention to cause harm constitutes an immoral infliction of damage under Section 1295(2) Austrian Civil Code (ABGB).

Liability also arises when such intention to harm does not exist (or cannot be proven) but a person had knowledge of the contractual obligation and deliberately influenced the will of the contracting party to breach the contract (see Austrian Supreme Court, Case 7 Ob 225/03v). According to the Austrian Supreme Court, in cases in which the initial buyer of an immovable object is not yet the owner, but already possesses the property, any secondary buyer becomes liable if they should have known that the seller is breaching its contract (see Austrian Supreme Court, Case 2 Ob 126/13p). However, the second buyer is only required to perform a limited amount of due diligence, as otherwise commercial transactions would be severely impaired. Liability for inducing the non-performance of an obligation is more restricted under German law. According to the prevailing view, the general clause in German tort law, Section 823(1) of the German Civil Code (BGB), only protects absolute rights. Hence, mere knowledge of a contractual obligation (which is a relative right) does not lead to liability for inducement of breaching an obligation. Only when the breach of contract was induced intentionally to cause harm to the contracting party and against good morals does liability arise according to Section 826 of the BGB.

While the level of care expected from downstream recipients of data under this Principle goes beyond the protection of contractual rights, it is significantly lower than the protection of absolute rights, such as ownership, which need to be respected by any third party. Other than under this Principle, the transferee of a movable object, even if it could not have had knowledge that the seller was not the owner of the sold object, infringes the owner's property rights. There are only a few exceptions, with rather strict requirements, to that general rule, most notably the acquisition in good faith, a doctrine that exists in all European legal traditions and is based on the rationale that the protection of the bona fide acquirer is necessary to ensure the functioning of commercial trade. In Austria, good-faith acquisition of movable goods is regulated in Section 367 of the Austrian Civil Code. The transferee acquires ownership of a good obtained from a person who is not the owner only if the transferee neither knows nor should suspect that the seller is not the owner, and the object is acquired either at a public auction, from a professional trader acting in the course of their ordinary business, or from a person to whom the owner voluntarily entrusted the object (*Vertrauensmann*). In France, transfer of ownership is based on a consensual system. Hence, ownership is transferred as soon as an express agreement to that effect is reached between both parties. In those cases, ownership is not transferred *solo consensus* but instead by mere possession. Excluded from good-faith acquisition are stolen and lost goods during a period of three years from the day of the loss or theft (Article 2276(2) French Code Civil). However, if the possessor of a lost or stolen thing has bought it in good faith at a fair, market, public sale, or from a merchant selling similar things, the possessor is only obligated to return the stolen or lost property to the dispossessed owner against reimbursement of the purchase price (Article 2277 French Code Civil). The German rules on good-faith acquisition (Sections 932 ff German Civil Code) require that the transferee obtained possession and does not know or has no reason to know that the thing does not belong to the transferor. However, good-faith acquisition is excluded if the goods were stolen from the owner or otherwise went missing and have not been bought in the course of a public auction (Section 935).

The Trade Secrets Directive (Directive (EU) 2016/943; see also Article 39 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)) also contains rules for onward

transfer. Those are less strict than the requirements for good-faith acquisition, but more far reaching than the liability for inducement of non-performance of an obligation. According to Article 4(4), the acquisition, use, or disclosure of a trade secret by a person is considered unlawful if the person knew or ought, under the circumstances, to have known that the trade secret was obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully within the meaning of Article 4(3) of the Directive. Article 4(3) states that the use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions: (a) having acquired the trade secret unlawfully; (b) being in breach of a confidentiality agreement or any other duty not to disclose the trade secret; (c) being in breach of a contractual or other duty to limit the use of the trade secret. While paragraph (1) of this Principle has certain similarities to Article 4(3), paragraph (2) of this Principle, unlike the Trade Secrets Directive, states a de minimis rule that limits the wrongfulness of data activities by a downstream recipient. The policy choice to include such a limitation was made because, otherwise, the protection of trade secrets would unjustifiably be extended to all types of data.

Similar effects vis-à-vis a downstream recipient can also be found in Articles 2(1)(xii) to (xv) of the Japanese Unfair Competition Prevention Act. Those provisions declare the act of disclosing shared data with limited access after having acquired it and learning that there had been an intervening act of wrongful acquisition of shared data with limited access to be "unfair competition." The same holds true for the act of using or disclosing the data that has been disclosed by an undertaking holding that data for the purpose of wrongful gain or causing damage to that holder of shared data with limited access. In addition, the act of acquiring shared data with limited access with the knowledge that the disclosure of that data is an act of improper disclosure of shared data with limited access, or that there has been an intervening act of improper disclosure of shared data with limited access with regard to the relevant shared data with limited access, or the act of using or disclosing shared data with limited access acquired in such a way, is declared to be unfair competition.

With regard to subsequent knowledge of unlawful activities, the rule laid down in the Trade Secrets Directive is also similar to paragraph (2)(b) of this Principle. According to Article 4(4) of the Trade Secrets Directive, unlawfulness of the acquisition, use, or disclosure of a trade secret is always determined "at the time of the acquisition, use or disclosure." Therefore, once the recipient knows or ought to know that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully, any further use becomes unlawful. Similarly, Article 2(1)(xvi) of the Japanese Unfair Competition Prevention Act qualifies the act of disclosing shared data with limited access after having acquired that data and learning that the relevant acquisition falls under an act of improper disclosure of shared data with limited access, or that there had been an intervening act of improper disclosure of shared data with limited access, as unfair competition. However, under this Principle, the subsequent knowledge does not lead to the unlawfulness of data activities by the downstream recipient if the recipient's reliance interests clearly outweigh, in the circumstances, the legitimate interests of a party protected under Principles 29 to 31.

CHAPTER C
EFFECTS OF OTHER DATA ACTIVITIES ON THE PROTECTION OF THIRD PARTIES

Principle 35. Duties of a Controller with regard to Data Processing and Derived Data

(1) If a controller may process data but is obligated to comply with duties and restrictions within the meaning of Chapter A, the controller must, when processing that data, exercise such care as is reasonable under the circumstances in:

(a) determining means and purposes of processing that are compatible with the duties and restrictions; and

(b) ascertaining which duties and restrictions apply with regard to the derived data, and taking reasonable and appropriate steps to make sure the duties and restrictions are complied with.

(2) Whether duties and restrictions with regard to the original data also apply with regard to derived data, or whether lesser or additional duties and restrictions apply, is to be determined by the rules and principles governing the relevant source of protection under Chapter A. In a case of doubt, considerations to be taken into account include:

(a) the degree to which the derived data is different from the original data, such as whether the original data can be reconstructed from the derived data by way of reasonable steps of disaggregation or reverse engineering; and

(b) the degree to which the derived data poses a risk for a protected party as compared with the risk posed by the original data.

(3) If processing the original data was not wrongful, but subsequent events occur that would make the same type of processing wrongful, this does not retroactively make the prior processing wrongful.

Comment:

a. General observations. Chapters A and B have addressed the question of when data activities are wrongful vis-à-vis a protected party, assuming that wrongfulness can be established with regard to a particular data set and that this data set remains more or less identical in the course of events, such as when it is supplied to a downstream recipient. In practice, however, this is rarely ever the case. Rather, data is usually subject to processing activities, meaning that data is structured, refined, or combined with other data, and new data is derived or inferred from existing data. This

makes the legal analysis much more complicated as it is unclear whether or to what extent the ground for wrongfulness is still present in the derived data, and, even if it is, investment has been made with respect to the data, and the data "tainted by wrongfulness" have been combined with "untainted" data. There may thus be situations in which it would be disproportionate and/or manifestly inefficient to judge data activities with regard to the processed data set in exactly the same way as data activities with regard to the original data set.

There are many different ways in which data may be processed. It is arguably not helpful to create different Principles for each typical processing activity, in particular as those activities are usually applied in combination, and as the lines between them are blurred. The main types of processing activities relevant for the purposes of Chapter C will be the structuring, aggregation, and analysis of data (including the drawing of inferences from data with the help of probabilistic or similar assumptions).

Illustration:

155. Credit scoring company B uses data it has been provided by, and that is about, customer C, who is seeking a loan, in order to obtain, with the help of a very complex algorithm, a figure representing C's credit score. Various steps may be involved here. Assuming B has collected data about C from different sources, and has combined and commingled them in sophisticated ways (e.g., representing, in a structured way, all information about C's conduct in the context of paying bills), that is aggregated data. If B has analyzed the input data and derived certain statistical data from it (e.g., that it took C, on average, 24 days to pay a bill that was due), that is derived data. If B then obtains the final credit score with the help of numerous probabilistic assumptions embedded in B's algorithm (e.g., that persons of C's age who take an average of 24 days to pay a bill, live in C's neighborhood, hold the same number of bank accounts and mobile phones as C does, and buy as much alcohol and coffee as C seems to according to payment services data, have a 34 percent probability of defaulting), B is generating inferred data. The aggregated, derived and inferred data all constitute "derived data" within the meaning of Principle 3(1)(i) and paragraph (1) of this Principle.

Often, data is used in such a way that inferences are drawn, but no inferred data is created and stored anywhere, so no inferred data seems to exist. Rather, the inference is drawn ad hoc with

the help of an algorithmic system, immediately triggering a reaction. This must have the same effect as if inferred data had been collected and stored.

Illustration:

156. In a scenario like the one described in Illustration no. 155, credit rating company B may in fact never calculate C's credit score (and store it in their system, later basing a recommendation to reject C's application for a loan on that score), but may instead apply an algorithm that, with the help of all the input data B has about C, automatically triggers the sending of a rejection letter. There are various reasons why B may prefer to do that, including circumventing data protection law. Nevertheless, the decision represented in the rejection letter would have the same effect as the inferred data, and would thus equally be covered by paragraph (1) of this Principle.

b. Duties of controller when processing. Any controller that intends to engage in processing of data with regard to which that controller is (or may be) bound by duties and restrictions under Chapters A and B must apply due diligence in making sure that processing the data in the intended way and for the intended purpose is compatible with the duties and restrictions. The level of diligence required depends, once more, on a risk-based assessment; that is, the higher the probability that restrictions may affect the processing, and the higher the potential risk for protected parties from noncompliance, the more inquiries a controller must make, and the more safeguards that the controller must put in place.

Illustration:

157. Credit rating company B in Illustration no. 155 not only calculates credit scores of consumers like C but also processes data generated by the smart heating system of its office building in order to cut down on repair and maintenance costs. The probability that data processing is subject to restrictions is considerably higher in the case of the consumer data than in the case of the heating system data, and so is the potential risk involved for third parties. Thus, B must apply a considerably higher level of diligence with regard to the consumer data.

After processing, the controller also must exercise reasonable care to ascertain which duties and restrictions apply with regard to the derived data. Often, the restrictions will be less strict than with regard to the original data because processing may have removed the basis for protection (e.g.,

previously personal data may have become anonymized). However, the opposite may also be true, in particular if data from different sources has been combined and risks for protected parties have increased.

Illustration:

158. Credit rating company B in Illustration no. 155 combines data of various types and from various sources, including data from fitness bracelets, step-counting apps, smart refrigerators, and shopping reward systems. All this data is combined for the purpose of making predictions concerning a consumer's health and consequential risk of becoming unemployed and defaulting on debts. The health-related data is much more sensitive than the input data from other sources, so more duties and restrictions might exist for processing the resulting health data than for processing the original data.

c. Prevailing duties and restrictions. When data undergoes processing, the legal situation with regard to that data changes, including, in particular, with regard to the protection of other parties under Chapter A. Duties and restrictions for the protection of such parties may be the same with regard to the derived data, or they may be lesser, or greater. Paragraph (2) of this Principle clarifies that the extent of these duties and restrictions is governed by those rules and principles that govern the duties and restrictions regarding the original data, or parts thereof. This is clear in the case of rights within the meaning of Principle 29, which are governed by particular bodies of law with their own inherent logic and principles.

Illustration:

159. Whether derived data in Illustration no. 155 counts as anonymous statistical data (such as the percentage of consumers living in a particular community defaulting on their debts) outside the scope of data protection law and without any restrictions on processing, or within the scope of such law, is to be determined exclusively by the applicable data protection law itself. The same holds true for the question of whether the health-related data in Illustration no. 158 is subject to stricter privacy rules and what those rules are.

However, the same holds true when limitations originate from contract within the meaning of Principle 30, in which case the exact scope of such limitations, and whether or not they extend to derived data, must normally be ascertained by way of contract interpretation.

Illustration:

160. Manufacturer M of machines transfers machine performance data to supplier C of an important component. C may not disclose "the data" to third parties. C processes the machine performance data and derives from that data, inter alia, data concerning the accuracy of performance measurement in general (which does not refer specifically to a particular type of machine). Whether this derived data is still covered by the contractual restriction on disclosing data to others, or whether this data is so different from the original performance data that C is free to use this data, is to be determined by contract interpretation.

d. Considerations in case of doubt. There may be cases in which the rules or principles ordinarily governing restrictions within the meaning of paragraph (1) are silent, or in which there are different possibilities of interpretation, and thus the default rule in paragraph (2) applies. Under this default rule, there are two cases in which duties and restrictions with regard to the original data, or part thereof, prevail with regard to derived data.

The first case is when the original data can, by reasonable reverse engineering, be reconstructed from the derived data. If the original data is more or less included in the derived data, the derived data obviously bears more or less the same inherent risks for protected parties as did the original data. The second case is when the duties and restrictions must be applied to the derived data to prevent harm to a party protected under Chapter A. The harm need not be exactly the same kind as the harm that might have followed from the original data.

Illustration:

161. Assume that the contract in Illustration no. 160 is silent as to the use of derived data, and a court needs to fill the gap. If a court concludes that disclosure of this data to third parties would not cause relevant harm to M, C may disclose this data to third parties without breaching its duty under this Principle.

e. Subsequent grounds for wrongfulness. Paragraph (3) of this Principle deals with situations in which processing data was rightful at the time it took place, but subsequent events make the same type of processing wrongful. Subject to any specific rule of law that exceptionally takes priority and provides for retroactive effect, these Principles suggest that such subsequent events should not normally affect the rightfulness of the processing. However, the subsequent

events may mean that the derived data is affected by the same grounds of wrongfulness, so any duties and restrictions that follow directly from Chapter A with regard to the derived data may be relevant and mean that the derived data must be deleted.

Illustration:

162. Assume that, under the applicable data protection law, processing of all consumer data in Illustration no. 155 was based on the consumer's consent. Assume further that, under the applicable data protection law, consent may be withdrawn at any time, and data whose control and processing relies exclusively on consent must normally be deleted. If consumer C withdraws consent, it makes future control and any future processing of the original data by B wrongful, but it also affects the derived data as far as this data is still identifiable to C.

Whether or not the subsequent grounds of wrongfulness affect the derived data is determined by paragraph (2).

REPORTERS' NOTES

United States:

Issues arising from when assets that are subject to a party's claims are aggregated with other assets raise legal problems in a number of contexts. See, e.g., in the context of security interests, Uniform Commercial Code (UCC) § 9-335 (2021-2022 ed.) (addressing accessions, and stating that security interests may be created in an accession) and UCC § 9-336 (addressing commingled goods, and stating that commingled goods may have security interests that do not exist for individual, unbundled goods).

Some statutes recognize practical limits on the ability to disaggregate personal information. For example, the California Privacy Rights Act added exemptions to the rights to delete personal information and to opt out of sharing of personal information if the consumer initially gave consent to the business's use of that personal information to produce a physical item containing the consumer's photograph, the business incurred expense in reliance on the consumer's initial consent, and compliance would not be commercially reasonable. CAL. CIV. CODE § 1798.145(r).

Europe:

a. General observations. The processing of data may in many instances lead to the generation of new data. To better illustrate the way in which the new data differs from the initial dataset, attempts have been made to categorize derived data according to the activity that gave rise to it. The terms "derived" data and "inferred" data are often used as synonyms for data that a controller creates by drawing conclusions from provided datasets (see Organisation for Economic Co-operation and Development (OECD), Enhancing Access to and Sharing of Data: Reconciling

Risks and Benefits for Data Re-use across Societies, 2019, p. 31; Japanese Ministry of Economy, Trade and Industry (METI), Contract Guidelines on Utilization of AI and Data – Data Section, 2018, p. 19; European Data Protection Board (EDPB), Guidelines 8/2020 on the targeting of social media users, Version 1.0, 2 September 2020, p. 22; see also Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10). Others, however, distinguish between data that has been derived and data that has been inferred. Derived data stems from a mechanical procedure on other data and is a new data element related to the individual. Inferred data implies the drawing of conclusions with the help of probabilistic or similar assumptions. In other words, the former is data that is simply derived in a fairly mechanical fashion from other data; the latter is the product of a probability-based analytic process (see Martin Abrams, The Origins of Personal Data and its Implications for Governance, 2014, p. 7 f.). In practice, it may be quite difficult to draw a clear line between derived and inferred data, which probably led to the custom to use these words as synonyms.

Another category that is frequently used is that of "aggregated data." While no universally accepted definition for "aggregated data" exists yet, it usually refers to the combination of initially separated data sets. Data aggregation is an activity that is likely to be conducted by controllers, as the value of the aggregated sets may significantly exceed the sum of values of the separate sets (Bertin Martens et al., Business-to-Business data sharing: An economic and legal analysis – JRC Digital Economy Working Paper 2020-05, 2020, p. 5, 12). However, the categorization as aggregated data does not indicate whether the combined datasets can, with reasonable effort, be disaggregated.

b. Duties of controller when processing and *c. Prevailing duties and restrictions.* Data that results from personal data is typically under the protection of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), as long as the derived data still relates to an identified or identifiable natural person and is thus considered personal data within the meaning of Article 4(1) of the GDPR. In determining whether a natural person is still identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, by the controller or another person, to identify the natural person directly or indirectly (see Recital 26 GDPR). If the derived data stems from data protected by the Trade Secrets Directive (Directive (EU) 2016/943), the infringer is required to destroy the data if it contains or embodies the trade secret (Article 12(1)(d)).

e. Subsequent grounds for wrongfulness. Subsequent grounds for wrongfulness typically do not affect any processing that has been made during the period before those grounds arose. The predominant example is the withdrawal of consent under Article 7(3) of the GDPR (Regulation (EU) 2016/679). While the data subject is entitled to withdraw his or her consent at any time, the provision explicitly sets out that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Principle 36. Wrongful Processing

(1) If processing data was wrongful, the controller must take all reasonable and appropriate steps to undo the processing, such as by disaggregating data or deleting derived data, even if duties and restrictions under Chapters A and B do not apply, in accordance with Principle 35, with regard to derived data.

(2) To the extent that undoing the processing in cases covered by paragraph (1) is not possible or would mean a destruction of values that is unreasonable in light of the circumstances giving rise to wrongfulness on the part of the controller and the legitimate interests of any party protected under Chapter A, an allowance may be made in money whenever and to the extent this is reasonable in the circumstances, and may be combined with restrictions on further use of the derived data. Factors to be taken into account include:

(a) whether the controller had notice of the wrongfulness at the time of processing;

(b) the purposes of the processing;

(c) whether wrongfulness was material in the circumstances or could be expected to cause relevant material harm to a party protected under Chapter A; and

(d) the amount of investment made in processing, and the relative contribution of the original data to the derived data.

(3) Paragraphs (1) and (2) apply with appropriate adjustments to products or services developed with the help of the original data.

Comment:

a. General observations. The question of the appropriate legal consequences of wrongful processing of data is one of the most complex issues in the data economy. Clearly, a balance needs to be struck between, on the one hand, the objective of encouraging negotiations and avoiding incentives for reckless infringement of others' rights (which might exist if a controller could fully keep and use the derived data), and, on the other hand, the objective of preserving value that has been generated. Under this Principle, the general rule is that a controller that has engaged in wrongful processing is under an obligation to undo the processing. However, as an alternative, a court may decide that the controller may make a monetary payment to the affected person, if requiring the controller to undo processing would be disproportionate and unreasonable in the circumstances.

It is important to understand the relationship between this Principle and Principle 35. When duties and restrictions for the protection of other parties within the meaning of Chapters A and B prevail with regard to the derived data, the legal consequences are those that follow from the relevant duties and restrictions themselves. This Principle only comes into play when, under Principle 35, duties and restrictions within the meaning of Chapters A and B do not apply to the derived data and therefore the controller would, but for this Principle, be allowed to keep the derived data. This Principle thus follows a "fruit of the poisonous tree" logic.

Illustration:

163. Social network provider P recklessly uses photographic material and stream recordings generated by its users for developing facial recognition artificial intelligence (AI). That use is clearly inconsistent with the applicable data protection regime. However, the resulting facial recognition AI does not, as such, qualify as personal data, and thus is not subject to any restriction following from data protection law. While P may be subject to a fine for having recklessly violated data protection law (if a regulator obtains sufficient evidence against P), P would—but for this Principle—still be able to use the facial recognition AI and benefit financially from it.

b. Duty to disaggregate, reverse-engineer, or delete. If data is processed wrongfully—whether because control of the original data was wrongful (e.g., because it was obtained by way of unauthorized access, see Principle 31) or because only the processing activities were wrongful (e.g., because the activities were excluded by way of contractual limitation, see Principle 30)—the controller normally must undo the processing. If the original data was wrongfully aggregated with other data, the controller is under an obligation to disaggregate the data (and, if control of the data was wrongful, subsequently give up any control of the relevant data after disaggregation). If derived data was wrongfully obtained by way of processing the original data, it qualifies as reverse-engineering (unless, if control was wrongful, the controller can delete both the original and the derived data). The same holds true for inferred data, which normally must be deleted if wrongfully obtained.

c. Limits on duty to disaggregate. Paragraph (2) of this Principle states that disaggregation, reverse-engineering, or deletion of data is not required to the extent that it is not possible or would mean a destruction of values that is unreasonable in light of the circumstances giving rise to wrongfulness on the part of the controller and the legitimate interests of any party protected under

Chapter A. If these conditions are met, an allowance may be made in money whenever and to the extent this is reasonable in the circumstances. Such an allowance may be combined with restrictions on further use of the derived data. What counts as "unreasonable" must be assessed in the circumstances, taking into account a number of factors. The list of factors provided in paragraph (2) is not exhaustive. It includes: (a) whether the controller had notice of the wrongfulness at the time of processing; (b) the purposes of the processing; (c) whether wrongfulness was material in the circumstances or could be expected to cause relevant material harm to a party protected under Chapter A; and (d) the amount of investment made in processing, and the relative contribution of the original data to the derived data.

Illustrations:

164. In the scenario described in Illustration no. 163, a court should take into account that social network provider P had notice of the wrongfulness and was acting recklessly, that biometric data is extremely sensitive data, and that, even if the resulting facial recognition AI does not refer to a particular individual, it affects particular groups of individuals in their fundamental rights, and that the purposes were purely commercial in nature. In such a situation, a court should not grant an exception under paragraph (2) of this Principle, even if P has made significant investment in the processing.

165. Company C wants to develop a new AI for helping combat a pandemic. For this purpose, C buys "anonymized" medical data from recognized medical service provider M. As C does not attempt to create any link between the data and any individuals, it escapes C's attention that, with advanced technological means and after combining the data with other data, an individual could theoretically be reidentified, so that the data counts as "personal data" within the meaning of the applicable data protection regime. In this case, a court should consider that C was acting in good faith, that the wrongfulness was not fundamental and there was no actual risk for data subjects, and that processing occurred for an important purpose. Therefore, a court might be inclined to grant an exception to the general obligation to undo the processing.

If the controller is not obligated under this Principle to undo the processing, Principle 35 still applies. It requires that, if the controller faces duties and restrictions with regard to the derived data, those duties and restrictions may still prevail.

Illustration:

166. If C in Illustration no. 165 does not use the data only to train AI (which is just software that does not allow any tracing back to particular training data) but also creates a database with the data, and puts it into open cloud space for health research, the database would consist of personal data, so the restrictions under the General Data Protection Regulation would still apply. If there is no legal basis for the processing, the database would still be "tainted" with the same problem as the original data.

d. Application with regard to products and services. If data is used for the generation of a product, including any digital content (such as software) or any design, or a service (such as a smart service), that product or service is no longer considered "data" within the meaning of these Principles. See Principle 3(1)(a). This is why paragraph (3) states that paragraphs (1) and (2) should be applied with appropriate adjustments when the result of processing is not (just) other data, such as aggregated, derived, or inferred data, but a product or service, such as AI. This also reduces the need to differentiate clearly between derived data and derived products or services.

Illustration:

167. The AI trained by C in Illustration no. 165 would not qualify as "data" within the meaning of these Principles, but rather as a "digital product." However, this Principle would apply with appropriate adjustments to the AI. If it would be an unreasonable destruction of value to destroy the AI, an allowance in money should be made to the protected party. The exact form of that allowance would, as a remedy, be determined by the applicable law in accordance with Principle 4(1).

REPORTERS' NOTES

United States:

Rights in derived data are largely analogous to "proceeds" from a particular asset. State law often defines "proceeds" as being part of wrongfully obtained property. See, e.g., CONN. GEN. STAT. ANN. § 56-36(a)(2). Moreover, a person with a security interest in a particular asset has a security interest in proceeds of that asset. Uniform Commercial Code § 9-315(a)(2) (2021-2022 ed.).

The right to derived data processed during a period of wrongful control is reflected in decisions regarding algorithms generated from wrongfully obtained data. Federal Trade Commission consent orders have required the deletion of all impermissibly obtained data as well as "any models or algorithms developed in whole or in part" using such data. See In re Everalbum,

Inc., File No. 1923172, at 2, 5 (F.T.C. Jan. 11, 2021), available at https://www.ftc.gov/system/files/documents/cases/everalbum_order.pdf. This represented a departure from prior consent orders that allowed companies to retain algorithms derived from illegally obtained data. See In re Google LLC & YouTube, LLC, File No. 1723083 (F.T.C. Sept. 10, 2019), available at https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf. Restitution applies to conscious interference with other protected interests, including the right to privacy, assuming disgorgement is susceptible of measurement, would not be inequitable, and would not conflict with limits imposed by other law. See Restatement of the Law Third, Restitution and Unjust Enrichment § 44 and Comment *b* (AM. L. INST. 2011). Claimants may obtain restitution from any products traceable to wrongfully obtained property. See Restatement of the Law Third, Restitution and Unjust Enrichment § 58 (AM. L. INST. 2011). Bona fide purchasers are exempt from equitable remedies. See id. § 66.

The right to derived data based on processing conducted before control became wrongful is likely to arise in conjunction with the consumer right to require deletion of personal data provided by some U.S. state statutes. See CAL. CIV. CODE § 1798.105; VA. CODE ANN. § 59.1-573(A)(3). In California, businesses may comply with requests for deletion by deidentifying or by aggregating the information. CAL. CODE REGS. tit. 11, § 999.313(d)(2).

Europe:

a. General observations, *b. Duty to disaggregate, reverse-engineer, or delete*, and *c. Limits on duty to disaggregate.* The duties under this Principle have certain similarities with Articles 12 f. of the Trade Secrets Directive (Directive (EU) 2016/943), Article 16(3) of the Digital Content and Services Directive (DCSD), Article 13(5) Consumer Rights Directive (CRD), and Article 11(3) of the proposal for a Data Act (COM(2022) 68 final).

If a trade secret has been unlawfully acquired, used, or disclosed, the competent judicial authorities may, at the request of the applicant, order one of the injunctions or corrective measures listed in Article 12 of the Trade Secrets Directive. Those measures include the destruction of all or part of any document, object, material, substance, or electronic file containing or embodying the trade secret. However, at the request of the person liable to be subject to measures (including erasure), the competent judicial authority may order pecuniary compensation to be paid to the injured party instead of applying those measures if all the following conditions of Article 13(3) of the Directive are met: (a) the person concerned at the time of use or disclosure neither knew nor ought, under the circumstances, to have known that the trade secret was obtained from another person who was using or disclosing the trade secret unlawfully; (b) execution of the measures in question would cause that person disproportionate harm; and (c) pecuniary compensation to the injured party appears reasonably satisfactory.

The DCSD and CRD exclude, in cases of termination or withdrawal by the consumer, obligations by the trader to return consumer-generated content when such content (a) has no utility outside the context of the digital content or digital service supplied by the trader; (b) only relates to the consumer's activity when using the digital content or digital service supplied by the trader; (c) has been aggregated with other data by the trader and cannot be disaggregated or only can be

disaggregated with disproportionate efforts; or (d) has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content (Article 16(3) DCSD; Article 13(5) CRD).

According to Article 11(2) of the Data Act proposal, when a data recipient abuses evident gaps in the technical infrastructure designed to protect the data of the data holder, uses the data for unauthorized purposes, or discloses the data to another party without the data holder's authorization, the recipient has to destroy the data made available by the data holder and any copies thereof (Article 11(2)(a)). The recipient also has to end the production, offering, placing on the market, or use of goods, derivative data, or services produced on the basis of knowledge obtained through such data, or the importation, export, or storage of infringing goods for those purposes, and destroy any infringing goods (Article 11(2)(b)).

The considerations underlying this Principle have some similarities to the doctrines of combination and commingling in the tangible world (for a comparative overview, see Brigitta Lurger and Wolfgang Faber, Principles for European Law - Study on a European Civil Code - Acquisition and Loss of Ownership in Goods, 2013, p. 1150 ff., 1180 ff.), even though this Principle does not follow the logic of property rights.

Those rules also set out the primary obligation to separate the resulting mass or mixture into its original constituents, as does paragraph (1) of this Principle. In this case, the initial owners simply remain owners of the respective parts and claim return based on general principles of ownership and possession. However, the consequences if it is impossible or economically unreasonable to separate the resulting mass or mixture are quite different from those provided in paragraph (2) of this Principle.

If goods owned by different persons are commingled and it is impossible or economically unreasonable to separate the resulting mass or mixture into its original constituents, but it is possible and economically reasonable to separate the mass or mixture into proportionate quantities, those persons become co-owners of the resulting mass or mixture, each for a share proportionate to the value of the respective part at the moment of commingling (Article VIII.-5:202 Draft Common Frame of Reference (DCFR): Article VIII.-5:202 Principles of European Law: Acquisition and Loss of Ownership of Goods (PEL Acq. Own.)).

The rules on combination under Article VIII.-5:203 of the DCFR and Article VIII.-5:203 of the PEL Acq. Own. provide that in the case that one of the component parts is found to be the principal part, the owner of that part normally acquires sole ownership of the whole, and the owner or owners of the subordinate parts are entitled, against the sole owner, to payment secured by a proprietary security interest in the combined goods. If none of the parts is to be regarded as the principal part, the owners of the component parts become co-owners of the whole, each for a share proportionate to the value of the respective part at the moment of combination. If, in the case of more than two component parts, one component part is of minimal importance in relation to other parts, the owner of that part is entitled, against the co-owners, only to payment proportionate to the value of the respective part at the moment of combination.

d. Application with regard to products and services. Paragraph (3) gives the protected parties under Chapter A similar protection as under the Trade Secrets Directive, which not only considers the acquisition, use, or disclosure of a trade secret unlawful, but also the production,

offering, or placing on the market of infringing goods, or the importation, export, or storage of infringing goods for those purposes (Article 4(5) Directive (EU) 2016/943).

Principle 37. Effect of Nonmaterial Noncompliance

(1) If a controller engages in data activities with respect to a large data set, and the data activities do not comply with duties and restrictions under Chapter A with regard to some of the data, the law should provide that such activities are not wrongful with regard to the whole data set if:

(a) the noncompliance is not material in the circumstances, such as when the affected data is only an insignificant portion of the data set with regard to which data activities take place;

(b) the controller made the efforts that could reasonably be expected in the circumstances to comply with the duties and restrictions; and

(c) the data activities are not related to the purpose for which duties or restrictions under Chapter A are imposed and could not reasonably be expected to cause material harm to a protected party.

(2) When paragraph (1) applies, the controller must, upon obtaining notice, remove the affected data from the data set for the purpose of future data activities unless this is unreasonable in the circumstances.

Comment:

a. General observations. The data economy is increasingly dealing with very large and diverse data sets. While the size and diversity of a data set does not in any way diminish the need for protection of third parties, it is becoming more difficult for players in the data economy to comply strictly with all duties and restrictions with regard to each and every data point they are controlling, including data points originally collected by others. The cumulative effect of legal regimes such as intellectual property protection, data privacy/data protection, trade secret protection, and contractual protection may well lead to a situation in which large data sets inevitably will contain some data points that are wrongful under one or another of those protective regimes. If the result of a minimal amount of such noncompliance is liability or other sanctions that are disproportionate to the magnitude of the noncompliance, overdeterrence may follow. For example, players in the data economy might no longer risk being transparent about their activities, and no longer share their data sets with others for the benefit of innovation and growth, because

they might be afraid that very minor acts of noncompliance could lead to disproportionate reactions. This could seriously endanger legitimate data activities that would ultimately be for the benefit of everyone.

In order to avoid such overdeterrence, this Principle provides that wrongfulness with respect to some items in a data set should not necessarily result in treating data activities with respect to the entire set as wrongful.

b. Criteria for application of this rule. Paragraph (1) of this Principle lists a number of criteria that must all be satisfied for the rule to apply. First, the rule applies only to large data sets in which data activities with regard to only an insignificant amount of the data are noncompliant with duties and restrictions under Chapter A. What constitutes "large" will necessarily depend on the context. The key element is that the noncompliance of the data activities must affect only an insignificant part of the data set, not the whole data set.

Illustration:

168. Huge amounts of data from connected cars, which are being controlled by car manufacturer M, qualify as personal data under an applicable data protection law. The owners of the cars, when first configurating their on-board computers, consented to certain data processing activities, but passengers, as to whom a comparatively minuscule amount of data has been collected, did not consent. Assuming that, under the applicable data protection law, data activities with respect to the data about the passengers is noncompliant with restrictions under Chapter A, a court might consider the noncompliance to be not material in the circumstances in light of the fact that the data from passengers amounts to only an insignificant portion of the overall data. In that case, the first criterion for application of paragraph (1) is satisfied.

The second criterion is the requirement under paragraph (1)(b) that the controller made efforts that could reasonably be expected in the circumstances to comply with the duties and restrictions. This criterion is satisfied even if unrealistic or unreasonable measures are theoretically possible.

Illustration:

169. In a situation such as that described in Illustration no. 168, assume that manufacturer M has taken all reasonable steps that could be expected in the circumstances,

including both steps to ascertain what its duties and restrictions are with regard to the data, and steps to avoid noncompliance. M is not required to take unrealistic or unreasonable measures, such as requiring car owners to obtain consent to data processing from all passengers.

The third criterion for application of the rule in paragraph (1)—that the type of data activity engaged in by the controller is not related to the purpose for which duties or restrictions within the meaning of Chapter A were imposed, and could not reasonably be expected to cause harm to a protected party—is important because it prevents application of the rule when the data activity in question may undermine the very reason for the restrictions.

Illustration:

170. In a situation such as that described in Illustration no. 168, the third criterion for application of the rule in paragraph (1) would not be satisfied if M's data activities were for the purpose of gaining insight particularly into how often passengers are taken for a ride, and how they behave with regard to the car. If, however, M's data activities were for training artificial intelligence (AI) with regard to how best to adjust the belt tension to a person's size, this data activity is not related to the purpose for which data protection restrictions were imposed, and no harm will be caused to a protected party. (Indeed, there is a possibility that the improved AI will also benefit those protected parties.)

c. Obligation to remove data upon request. While application of the rule in paragraph (1) protects the controller from a claim that its activities with respect to an entire data set are wrongful when the controller's wrongful data activities are not material, this should not mean that the controller may continue to engage in the same type of data activities with the affected data. Accordingly, paragraph (2) provides that when a controller's data activities are noncompliant, the controller must still remove the affected data from the data set for future processing upon request by a protected party unless removal would be unreasonable in the circumstances.

Illustration:

171. Assume that, in a situation such as that described in Illustration no. 168, passenger P learns about M using passenger data for training its belt tension AI and requests M to remove P's personal data from the data set. If this can be done easily without burdensome and expensive efforts, M must comply with the request.

d. Relationship to other law. This Principle is, of course, subject to contrary doctrines in data protection/data privacy law, intellectual property law, etc.; see Principle 1(2). Nonetheless, this Principle serves important purposes. First, Chapter A addresses not only protection arising from those bodies of law but also from other areas such as contract law. Second, even the areas of law to which these Principles defer may not fully address these issues, in which case this Principle may serve as a gap filler. Third, to the extent that those areas of law evolve and develop, this Principle may provide a useful source of factors to consider in that process.

REPORTERS' NOTES

United States:

U.S. law frequently distinguishes between substantial performance of duties on the one hand and material breach of duties on the other hand. In the context of installment contracts, for example, see Uniform Commercial Code § 2-612 (2021-2022 ed.). More generally, see, e.g., Restatement of the Law Second, Contracts § 237 (AM. L. INST. 1981) ("it is a condition of each party's remaining duties to render performances to be exchanged under an exchange of promises that there be no uncured material failure by the other party to render any such performance due at an earlier time"). A well-known case examining this concept is Jacob & Youngs v. Kent, 129 N.E. 889 (N.Y. 1921). See also Lovink v. Guilford Mills, Inc., 878 F.2d 584, 587 (2d Cir. 1989).

Europe:

a. General observations. If a data set covers data protected by third party rights, those third-party rights typically apply to the whole set of data if it is not possible to separate the affected data. For example, according to Article 2(2) of the Free Flow of Data Regulation (Regulation (EU) 2018/1807), the General Data Protection Regulation (GDPR) shall apply when the data set contains personal data that is inextricably linked with the non-personal data. The European Commission has further specified that the GDPR shall apply regardless of the extent to which personal data are included in mixed datasets. Hence, the GDPR applies even if the personal data only represents a marginal share of the aggregated data (COM(2019) 250 final, p. 9).

b. Criteria for application of this rule and *c. Obligation to remove data upon request.* In contrast to the Free Flow of Data Regulation, this Principle sets out that wrongfulness with respect to some items in a data set should only result in treating data activities with respect to the whole data set as wrongful, if the criteria in paragraphs (1)(b) and (1)(c) are also fulfilled. These partly overlap with the criteria set forth in Principle 36, which is why reference is made to the Reporters' Notes to Principle 36.

PART V
MULTI-STATE ISSUES

Principle 38. Application of Established Choice-of-Law Rules of the Forum

(1) When an issue is within the territorial scope of the law of more than one state, the law applicable to that issue is determined by the forum's choice-of-law rules. These Principles do not determine the territorial scope of a state's law.

(2) The law applicable to data contracts under Part II should be the law of the state that would be selected under the forum's choice-of-law rules for contracts.

(3) For any other issue arising under these Principles, the law applicable to that issue should be:

(a) the law of the state that would be selected under the forum's choice-of-law rules if those rules provide a clear rule for determining the law applicable to that issue; or

(b) if the forum's choice-of-law rules do not provide a clear rule for determining the law applicable to that issue, the law determined by application of Principle 39.

Comment:

a. General observations. The characteristics of digital data are such that there are few natural barriers to cross-border data transactions. Modern forms of electronic communication make it easy for the parties to such a transaction to communicate with each other, and data controlled by a party in one state can easily be transferred to a party in another state or be accessed by a party in another state. While legal relationships concerning data are already very complex in a purely domestic setting, the analysis of rights and duties of the parties is even more complex when the parties are in different states inasmuch as rights and duties may be different in one state than in the other. When a matter touches more than one state, differences between the law of one of the states and that of another are resolved by application of the forum's choice-of-law rules.

This Principle should be understood as saying that courts or other authorities may continue to use existing, clear approaches to resolving potential choice-of-law issues with regard to matters addressed by these Principles. It also clarifies that Part V of these Principles does not deal, in particular, with how the territorial scope of a state's regulatory regimes should be defined. These

Principles do not cover the possible interactions of regulatory regimes in a particular forum. Those are each issues for determination by the forum, and will depend on a number of factors that differ from jurisdiction to jurisdiction, including mandatory application and the territorial extent of that application.

b. Deferral to the choice-of-law rules of the forum for contract issues. Most states have well-developed choice-of-law rules to determine which law governs certain relationships with an international (or, in a federal system such as the United States, an interstate) element. This holds true, in particular, for contracts, including the data contracts addressed in Part II. These rules (which may vary depending on whether or not the parties have agreed on what law is to govern their contract and whether the contract is between businesses or a consumer is involved) are typically general in nature and apply across a wide range of contracts. Paragraph (1) of this Principle recommends that a forum apply those general choice-of-law rules to data contracts rather than devise a special rule for data transactions.

Choice-of-law rules in most states give the parties to a cross-border contract substantial leeway to select the law governing their contract. In business-to-business transactions, many states allow the parties to a cross-border contract to select the law of any state to govern their contract, subject only to fundamental notions of public policy of the forum (or of another state whose law would be applicable in the absence of a choice of law by the parties) or application of an overriding mandatory provision of the forum's law. Other states similarly allow the parties to a cross-border transaction to select the state whose law will govern that contract, but limit that choice to the selection of a state that bears some sort of relationship to the parties or the contract. States vary as to the ability of parties to select the governing law in contracts with consumers, with some states reducing the range of possible choices in some contexts.

Illustration:

172. Company S, established in State X, sells a large data set to company R, established in State Y. S and R agree to have their contract governed by the law of State X. If a dispute arises and is litigated in the courts of State Y, and the choice-of-law rules of State Y give effect to the parties' choice of the applicable law, the contract will be governed by the law of State X.

When the forum's choice-of-law rules are applied in a context in which the law of one or more states regulates an area of substantial public concern rather than simply allocating private

rights, the role of overriding mandatory provisions of the forum's law may increase and sometimes result in application of the forum's law to a particular topic without regard to the law of other states whose law might otherwise apply. In such a context of substantial public concern, in which the public policies of states may differ significantly, it is also possible that, when application of a forum's choice-of-law rule initially refers a matter to the law of another state, the law of that other state may be manifestly incompatible with fundamental notions of public policy of the forum (or of another state whose law would be applicable in the absence of a choice of law by the parties) and, therefore, its application to the matter will be excluded.

c. Deferral to the choice-of-law rules of the forum for other issues as to which the forum state has clear rules. While existing choice-of-law rules for contracts apply directly to data contracts within the meaning of Part II (as they would apply to contracts unrelated to data), the situation is a bit different with other legal issues addressed by these Principles, notably with data rights under Part III, and in particular rights in co-generated data. Such data rights are not yet an established area of the law in most legal systems, with the possible exception of open data in the public sector. Similarly, most legal systems do not have clear and well-established conflict-of-laws rules with respect to data rights (or more general concepts that map onto data rights).

For states that do have such rules, or develop them in the future by creating new paradigms or integrating rules with respect to data rights into existing and well-established frameworks, such as contract law, tort law, property law, or competition law, this Principle recommends deferral to them.

Illustrations:

173. Small airline A operates airplanes manufactured and sold by P, the engines for which were supplied by engine manufacturer E. Data concerning the performance of the engines is transmitted directly from the connected engines to D, a data-analytics company developing predictive maintenance services and belonging to the same group of companies as E. A would like to have access to the engine data in order to get a better idea of whether maintenance could be dealt with in a more cost-efficient way. A court in State X is confronted with the question of whether airline A has a right against D to be provided with access to the data, and the law of the relevant states differ so that the court must determine which state's law is applicable. If the choice-of-law rules of State X provide clear rules to

determine which state's law governs matters addressed in Part III of these Principles, those choice-of-law rules should be applied by the court to determine the applicable law.

174. Company S established in State X sells goods over the online marketplace run by platform provider P established in State Y. A dispute arises as to whether S, which seeks to move to another online marketplace run by Q, has a right against P to have S's reputational data from customer reviews transferred to Q. If, according to the choice-of-law rules of the forum, the law of State Y clearly governs matters of competition, and if the law of State Y has implemented access rights in co-generated data in competition law, those parts of the competition law of State Y would apply.

The same considerations apply to other legal issues addressed, directly or indirectly, by these Principles and for which established choice-of-law rules exist, such as for intellectual property protection and infringements of intellectual property rights, which are not dealt with by these Principles but are addressed as given under Part IV. Similarly, if, under a clear and well-established approach, the courts of the forum state apply a particular regulatory regime of that state to all matters that are within the territorial scope of that regulatory regime, paragraph (3)(a) of this Principle recommends that that approach should continue to be followed.

For states that do not have choice-of-law rules that provide clear guidance for determining the law applicable to an issue, Principle 39 identifies several factors to be used in choice-of-law analysis.

REPORTERS' NOTES

United States:

For U.S. choice-of-law principles applicable to contracts, see Restatement of the Law Second, Conflict of Laws, Chapter 8 (AM. L. INST. 1971). Party autonomy to select the law governing a contract is addressed in Restatement of the Law Second, Conflict of Laws § 187 (AM. L. INST. 1971). General principles that determine the applicable law in the absence of an effective choice by the parties are addressed in Restatement of the Law Second, Conflict of Laws § 188 (AM. L. INST. 1971). See also Restatement of the Law Third, Conflict of Laws §§ 8.01 and 8.02 (Council Draft No. 5, 2021).

The Hague Principles on Choice of Law in International Commercial Contracts (HCCH Principles) apply when the contract is international and when the parties act in the exercise of their trade or profession. A contract is "international" within the HCCH Principles unless the parties have their establishments in the same state and the relationship of the parties and all other relevant elements, regardless of the chosen law, are connected only with that state (Article 1(2)).

Furthermore, each party to the contract must be acting in the exercise of its trade or profession. These Principles expressly exclude from their scope certain specific categories of contracts in which one party—such as a consumer or employee—is presumptively in a weaker bargaining position, e.g., consumer and employment contracts (Article 1(1)). According to the HCCH Principles, international contracts within those Principles are governed by the law chosen by the parties (Article 2(1)). The choice of law must either be explicit or appear clearly from the provisions of the contract or the circumstances (Article 4). However, the HCCH Principles do not require a connection between the law chosen and the parties or their transaction (Article 2(4)). The law chosen by the parties shall govern all aspects of the contract between them, including but not limited to (a) interpretation; (b) rights and obligations arising from the contract; (c) performance and the consequences of nonperformance, including the assessment of damages; (d) the various ways of extinguishing obligations, and prescription and limitation periods; (e) validity and the consequences of invalidity of the contract; (f) burden of proof and legal presumptions; and (g) pre-contractual obligation (Article 9). However, the HCCH Principles shall not prevent a court from applying overriding mandatory provisions of the law of the forum that apply irrespective of the law chosen by the parties (Article 9(1)). A court may exclude application of a provision of the law chosen by the parties only if and to the extent that the result of such application would be manifestly incompatible with fundamental notions of public policy (*ordre public*) of the forum (Article 9(2)).

U.S. law lacks a uniform rule governing choice of law. Most states have adopted the Restatement of the Law Second, Conflict of Laws (AM. L. INST. 1971), while others have adhered to the first Restatement of the Law, Conflict of Laws (AM. L. INST. 1934), and still others have adopted a hybrid approach. Both § 6 of the Restatement Second and § 7 of the first Restatement endorse the approach adopted by this Principle, which provides that courts should resolve choice-of-law issues under forum law. Courts have applied the forum's choice-of-law rules to contracts for data. In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1167-1168 (N.D. Cal. 2016); Peterson v. Martinez, No. A17-0355, 2017 WL 6418224, at *4 (Minn. Ct. App. Dec. 18, 2017).

Section 187 of the Restatement Second explicitly endorsed the application of choice-of-law clauses in contracts, deviating from the first Restatement's hostility toward the practice. Restatement of the Law Second, Conflict of Laws § 187 (AM. L. INST. 1971). Even states that adhere to the first Restatement approach have generally adopted a policy of favoring the enforceability of choice-of-law clauses.

Section 188 of the Restatement Second lays out the principles that determine the applicable law in the absence of a choice-of-law clause. Restatement of the Law Second, Conflict of Laws § 188 (AM. L. INST. 1971). That Section identifies the key question of which state has the most significant relationship to the transaction and the parties, and five specific types of contacts that courts should take into account when making that determination.

Europe:

a. General observations. In Europe, there are different approaches to resolving a potential conflict of laws, including any regulatory regimes of two or several states whose law might be applicable in a cross-border situation. First and foremost, there may be legal provisions applicable

in the forum state that directly and specifically address cross-border situations, including by way of international uniform law, such as the United Nations Convention on the International Sale of Goods (CISG). Secondly, for a number of regulatory regimes, there may be specific rules defining the territorial scope of the regulatory regime. When this is the case, a national court or other authority that has assumed jurisdiction would normally not even consider the application of foreign law, but simply apply the regulatory regime to any situation that is within the territorial scope of that regime. This method is used for a broad range of legal instruments that are commonly considered "data law," including the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), the Free Flow of Data Regulation (Regulation (EU) 2018/1807), and the Platform-to-Business Regulation (Regulation (EU) 2019/1150), as well as the future E-Privacy Regulation (Commission Proposal COM(2017), 10 final), Data Governance Act (Regulation (EU) 2022/868), Digital Services Act (ST 9342 2022 INIT), Digital Markets Act (ST 8722/2022 INIT), AI Act (COM(2021) 206 final), and the proposal for a Data Act (COM(2022) 68 final). In some legal instruments, such as the Open Data Directive (Directive (EU) 2019/1024, or, rather, national law implementing the Directive) and much of sectoral legislation, rules on territorial scope are more implicit. Thirdly, legal instruments may also explicitly or implicitly mandate the recognition (or, in fact, non-recognition) of certain foreign elements, e.g., in areas in which the GDPR leaves a degree of leeway to the Member States, and thus the requirements may differ from state to state when it is held that a controller engaging in cross-border data activities only needs to fulfill the requirements of their own state (see Recital 153, 6th sentence, GDPR), although the matter is still disputed. Fourthly, as far as a matter is governed by the more traditional areas of what is often considered to be "private law," such as contract and tort law, but also intellectual property law or competition law, the forum's choice-of-law rules (which, in turn, may be of international, EU, or domestic origin) would designate the applicable law by way of connecting factors and a range of specific choice-of-law methods and doctrines (such as classification, *dépeçage*, *renvoi*, assimilation, or *ordre public*). It is only in the context of the fourth (and, to a certain extent, the third) of the four approaches explained above that a court or other authority would genuinely consider the "application" of foreign law, but even in that situation there are different views as to what extent the foreign law is genuinely applied as law (for example, in Germany, see Reinhold Geimer, Internationales Zivilprozessrecht, 7th Edition, 2015, p. 963 f, and in France, see Cass. Civ. 18.9.2002, Bull. Civ. I Nr. 2) or more as fact (for example, in the UK, see *Bumper Development Corpn*. v. *Comr. of Police* [1991] 1 W.L.R. 1362, 1368). Only as far as paragraph (1) of this Principle states that courts or other authorities may continue using existing, clear approaches to resolving potential choice-of-law issues, it refers to all four approaches just described. However, it also clarifies that Part V of these Principles does not deal, in particular, with how the territorial scope of regulatory regimes should be defined (i.e., it does not give any specific guidance with regard to the third approach).

b. Deferral to the choice-of-law rules of the forum for contract issues. In Europe, data contracts under Part II are governed by the Rome I Regulation, which lays down rules on the conflict of laws for contractual obligations in civil and commercial matters (Article 1(1) of Regulation (EC) No 593/2008). A contract shall generally be governed by the law chosen by the parties. The choice of law can be made expressly or be clearly demonstrated by the terms of the

contract or the circumstances of the contract (Article 3). In Articles 5 to 8, the Regulation lays down rules for the law applicable to contracts of carriage, consumer contracts, insurance contracts, and individual employment contracts. If the applicable law is not chosen and none of Articles 5 to 8 apply, the law governing the contract shall be determined by Article 4(1) of the Regulation, which specifies the law applicable to certain contracts. The list of contracts specifically mentioned includes sales contracts (Article 4(1)(a)), service contracts (Article 4(1)(b)), and the sale of immovable property (Article 4(1)(c)). If the contract is not covered by the specific rules of Article 4(1), or if the elements of the contract would be covered by more than one point, the contract is governed by the law of the country where the party required to effect the characteristic performance of the contract has its habitual residence (Article 4(2)). However, if it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than one indicated in Article 4(1) and (2), the law of that country shall apply instead (Article 4(3)). When the law applicable to the contract can still not be determined, the contract is governed by the law of the country with which it is most closely connected (Article 4(4)).

The Rome I Regulation follows the rule introduced by its predecessor, the Rome Convention, that the contract is governed by the law of the state where the party required to effect the characteristic performance of the contract has its habitual residence. For most contracts for supply or sharing of data under Part II, Chapter B, the characteristic performance is not the remuneration paid by the recipient, but the performance by the supplier. Therefore, the rules set out in Article 4(1) or (2) of the Rome I Regulation will generally lead to the application of the law of the country in which the supplier has its habitual residence. This may be different for contracts for authorization to access data under Principle 10, as authorization to access is often provided in lieu of a consideration in money, such as in many mass contracts for digital content or digital services. In those cases, the characteristic performance will be the supply of the digital content or service. When such cases involve consumer contracts, the special rules under Article 6 take priority, which often lead to the application of the law of the consumer's habitual residence. Contracts for data pooling within the meaning of Principle 11 will often be governed by the law of the otherwise closest connection according to Article 4(4), unless rules of international company law come into play.

Contracts for services with regard to data (Part II, Chapter C) would fall under the broad notion of "contracts for the provision of services" under Article 4(1)(b) of the Regulation that applies to activities in return for remuneration (see CJEU, Case C-533/07 ECLI:EU:C:2009:257 – *Falco Privatstiftung*). Thus, the law of the country where the service provider has its habitual residence applies.

c. Deferral to the choice-of law-rules of the forum for other issues as to which the forum state has clear rules. In Europe, the law applicable to data rights under Part III is primarily determined by the choice-of-law rules and similar rules in existing specific legislation (see Christiane Wendehorst, in Jürgen Säcker/Roland Rixecker/Hartmut Oetker/Bettina Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 13 – Internationales Privatrecht, 2020, Art. 43 EGBGB no. 297 f.). Apart from the many instances in which a matter will be dealt with by a regulatory regime that defines its own territorial scope (see the Reporters' Notes to Comment *a*), this will typically lead to the application of the Rome I and the Rome II Regulations

where data rights have been implemented in a framework of contractual or non-contractual obligations.

The Rome II Regulation (Regulation (EC) No 864/2007) governs non-contractual obligations, such as obligations arising out of a tort/delict. As a general rule, the Regulation leads to the application of the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurs and irrespective of the country or countries in which the indirect consequences of that event occur (Article 4(1)). But when the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply (Article 4(2)).

However, data rights may be implemented under competition law or intellectual property law, for which the Rome II Regulation provides specific rules in Articles 6 and 8, which take priority over the general rule in Article 4.

As to obligations arising out of acts of unfair competition, the Rome II Regulation differentiates between market-related and competitor-related acts. If the act in question affects the public, i.e., is a "market related act," Article 6(1) provides for the law of the country where the interests protected by the law of unfair competition are affected. However, if the act only affects the interests of a specific competitor, i.e., is a "competitor-related act," Article 6(2) refers to the general rule of Article 4, and thus the usual rules on the law applicable to obligations arising from tort/delict apply. In contrast, the law applicable to a non-contractual obligation arising out of a restriction on competition is determined by the "market effects principle," which leads to the application of the law of the country whose market is, or is likely to be, affected (Article 6(3)(a)).

European intellectual property law is dominated by the *lex loci protectionis*, which is stated in Article 8(1) of the Rome II Regulation. The law applicable to a non-contractual obligation arising out of an infringement of an intellectual property right is the law of the country for which protection is claimed. While this is unproblematic in single-state scenarios, it leads to the application of the laws of all countries for which the plaintiff claims protection if an act of infringements affects intellectual property rights in a number of countries (the so-called "mosaic approach").

It is important to note that the Rome II Regulation excludes certain obligations from its scope, among them obligations arising out of violations of privacy and rights relating to personality (Article 1(2)(g) Rome II Regulation), and obligations arising from an infringement of the GDPR. Given that claims for damages under the GDPR may follow slightly different rules from jurisdiction to jurisdiction, it may be important to determine which law of damages applies. However, the GDPR does not contain any detailed choice-of-law rules. This was not the case under the previous data privacy regime with the Data Protection Directive (Directive 95/46/EC), which provided for application of the law of the country to which the activities of the controller were directed, if the controller carried out the data processing in question in the context of the activities of an establishment situated in that country (Case C-191/15 ECLI:EU:C:2016:612 – *Verein für Konsumenteninformation* v *Amazon EU Sàrl*). However, it is unclear to what extent this judgment is still relevant in determining the applicable national law under the GDPR. It is more convincing to conclude from Recital 153 of the GDPR, which basically refers to the law of the Member State to which the controller is subject in the context of freedom of expression (see also Article 6(3)(b);

Article 23 GDPR), that the law of only *one* country should apply. That would mean that the GDPR, at least for intra-European choice-of-law conflicts, generally follows the country-of-origin rule (Marian Thon, Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO, 2019 *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, p. 24, 44 f.).

Principle 39. Issues Not Covered by Established Choice-of-Law Rules of the Forum

(1) The law applicable to issues not already covered by Principle 38 should be the law of the state that has the most significant relationship to the legal issue in question. Contacts to be taken into account in determining which state has the most significant relationship include:

(a) the place where data activities

(i) are designed to produce effects on relevant interests, or

(ii) actually produce effects;

(b) the domicile, residence, nationality, place of incorporation, and place of business of the party asserting a right and the party against whom it is asserted; and

(c) the law of the state that governs a preexisting legal relationship, if any, between the party asserting a right and the party against whom it is asserted; and

(d) the place where the data is generated.

(2) Parties may, by mutual agreement made after a dispute has arisen, choose the state whose law will govern their legal relationship with regard to a legal issue addressed by these Principles, unless this is incompatible with the nature of the legal issue or considerations of public policy.

Comment:

a. General observations. While conflict-of-laws issues with respect to contract matters are covered by Principle 38(2), and conflict-of-laws issues with respect to other issues may be covered by Principle 38(3), there may be legal issues relating to data with regard to which the forum state does not provide clear, established choice-of-law rules. This Principle provides guidance as to the factors to be taken into account in making conflict-of-laws decisions for those issues.

b. Most significant relationship. If the law applicable to an issue related to data is not determined by application of the choice-of-law rules referred to in Principle 38, this Principle recommends that the legal issue be governed by the law of the state that has the most significant relationship to that issue. Paragraph (1) of this Principle lists four categories of contacts to be taken

into account in determining which state has the most significant connection to the issue. Each of those categories is worthy of consideration in a choice-of-law determination.

First, it is appropriate to consider the place where data activities are designed to produce effects, or where they actually produce effects. The second connecting factor relates to the location of the parties, inasmuch as the states in which they are located have an obvious interest in application of their legal rules.

Illustration:

175. A drives a connected car in Austria, his home state. He bought the car from retailer B in Germany. The data collected by the connected car is controlled by U.S. manufacturer M. For purposed of maintenance for the car, A seeks access to the data under Principle 20. When determining the law applicable to any access right A may have against M, the court should consider that the data has been generated in Austria, that data processing has serious effects on maintenance to be carried out in Austria, and that the residence of A is in Austria, while M's place of business is in the United States.

Thirdly, paragraph (1)(c) provides that the law governing a preexisting legal relationship should be taken into account when assessing which state has the most significant relationship with the data right at issue.

Illustration:

176. If A and M in Illustration no. 175 have some form of relationship, for example, stemming from an end user license contract, the law applicable to that relationship should also play a role when determining the most significant relationship of the data right asserted by A against M. However, the sales contract with B should not be considered because it is a legal relationship with a different party.

Last but not least, and particularly with regard to data rights that arise out of the generation of data (i.e., rights in co-generated data under Chapter B of Part II), it is appropriate that a connecting factor be the place or places where the data was generated, which is typically the place where the activity that led to the generation of the data occurred.

c. Choice of applicable law by the parties. Paragraph (2) permits the parties to choose, by mutual agreement made after a dispute has arisen, the state whose law will govern their legal relationship with regard to a legal issue addressed by these Principles, unless this is incompatible

with the nature of the legal issue or considerations of public policy. After the litigation begins, the parties should have the ability to enter into contracts that simplify resolution of their dispute and make outcomes more predictable. Also, the opportunity to try the case under an agreed law allows a court to clarify the disputed issues more expeditiously.

REPORTERS' NOTES

United States:

With respect to choice of law, compare the general U.S. policy regarding choice of law, in which the factors relevant to the choice of applicable law include: (a) the needs of the interstate and international systems; (b) the relevant policies of the forum; (c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue; (d) the protection of justified expectations; (e) the basic policies underlying the particular field of law; (f) certainty, predictability, and uniformity of result; and (g) ease in the determination and application of the law to be applied. Restatement of the Law Second, Conflict of Laws § 6 (AM. L. INST. 1971).

The problems addressed in this Principle are analogous to those addressed in Restatement of the Law Second, Conflict of Laws, Chapter 9, Topic 3 (Movables) (AM. L. INST. 1971).

Paragraph (1) is similar to the general principle laid out in Restatement of the Law Second, Conflict of Laws § 222 (AM. L. INST. 1971), which provides that choice of law turns on which state "has the most significant relationship to the thing and the parties."

Courts have relied on factors similar to those in paragraph (1) when finding sufficient contacts with a state to justify permitting out-of-state plaintiffs to assert data rights created by that state's statutes. In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 486 (D. Minn. 2015).

Paragraph (2) recognizes that parties may enter into choice-of-law agreements with respect to data rights. Such choice-of-law clauses are limited by Restatement of the Law Second, Conflict of Laws § 187(2) (AM. L. INST. 1971), which supports enforcement of such clauses unless (a) "the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice" or (b) "application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue." Applying those principles, courts have overridden a choice-of-law clause when enforcing that clause would be contrary to another state's fundamental policy and the other state has a greater interest in the outcome of the dispute. In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1168-1170 (N.D. Cal. 2016). As for choice-of-law clauses entered into after a dispute has arisen, see, e.g., Principles of the Law, Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes § 302(1) (AM. L. INST. 2008) ("the parties may agree at any time, including after a dispute arises, to designate a law that will govern all or part of their dispute.").

Europe:

a. General observations. See the Reporters' Notes to Principle 38, Comment *a*. In particular, it is important to stress that this Principle only applies insofar as the forum takes a "connecting factor approach" to resolving a potential conflict of laws, but does not give any guidance with regard to the territorial scope of a regulatory regime.

b. Most significant relationship. The "closest connection" is a guiding principle in European private international law and stated, e.g., in Article 4(4) of the Rome I Regulation (Regulation (EC) No 593/2008: "Where the law applicable cannot be determined pursuant to [Articles 4(1) and (2)], the contract shall be governed by the law of the country with which it is most closely connected") and Article 4(3) of the Rome II Regulation (Regulation (EC) No 864/2007: "Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in Articles 4(1) or (2), the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.").

c. Choice of applicable law by the parties. Parties to non-contractual obligations are generally free to submit their legal relationship to the law of their choice by an agreement entered into after the event giving rise to the damage occurred, or, when all the parties are pursuing a commercial activity, by an agreement freely negotiated before the event giving rise to the damage occurred (Article 14 (1) Rome II Regulation). However, with regard to infringements of intellectual property rights or non-contractual obligations arising out of an act of unfair competition, parties may not deviate from the rules on international private law (see Article 6(4) and 8(3) Rome II Regulation).

Principle 40. Relevance of Storage Location

(1) Except as provided in paragraph (2), for choice-of-law purposes, the location of the storage of data is relevant as a connecting factor only when the issue in question relates to storage or to rights in the medium.

(2) The location of storage of data may be relevant for choice-of-law purposes as a connecting factor of a residual nature, such as in the absence of other connecting factors or when consideration of other connecting factors is indeterminate.

(3) The fact that data is stored outside a state does not of itself ordinarily raise issues of extraterritorial exercise of jurisdiction or application of law as long as there are sufficient links between the state and the activities with respect to the data it seeks to regulate or the entitlements with respect to the data it seeks to enforce.

Comment:

a. The limited role of territorial location of data storage and of physical establishment. Data can move across the globe within fractions of a second; different parts of files and other meaningful units of data may be stored in different territories; and data may be accessed and processed remotely from all parts of the world. All of this results in disconnection between the territorial location of data storage and any link to meaningful activities carried out with regard to data and the impact of those activities. While providing a comprehensive set of choice-of-law principles or principles concerning territorial reach of jurisdiction and substantive law rules for legal relationships involving data is beyond the scope of these Principles, this Principle provides that the territorial location of data storage is normally not relevant.

b. Choice of law. If the law of more than one state might be applied to a particular issue, courts must decide which state's law to apply. In many instances, in particular with regard to contractual obligations, a choice of the applicable law made by the parties themselves will be given effect by the courts. In many cases, however, the parties have not made a choice, or the issue at hand is of such a nature as to prevent courts from giving effect to a choice by the parties. In that case, choice-of-law rules and doctrines typically look to the law of the state with the most significant contacts with the matter. This Principle makes clear that the location of storage of data is ordinarily not a significant contact with respect to an issue unrelated to that storage.

Illustration:

177. Company G established in State 1 has customer data stored in cloud space provided by F. F is established in State 2, but operates servers in States 3 and 4. Hacker H, who operates from State 5, manages to gain access to the data stored on the servers. In determining the law governing G's claim against F and/or H for damages, the location of the servers in States 3 and 4 should not be considered as a significant contact.

Exceptionally, the location of data storage may be relevant to choice of law if the rights and remedies in question have a specific link with storage as such or with the rights in the medium.

Illustration:

178. Same situation as in Illustration no. 177, but F takes recourse against the local provider of the server in State 4. This dispute is related to storage as such; therefore, the fact that the servers are located in State 4 is relevant for determining the applicable law.

c. Storage location as connecting factor of residual nature. While ordinarily the location of storage is not a relevant connecting factor except when the issue in question has a specific link to storage or to the rights in the medium, courts may treat the location of storage as relevant when the weight of other connecting factors is so similar as to make a determination of which law to apply very difficult. In such a case, the territorial location of data storage may have some very limited significance of a more residual nature, such as when a court has to determine the closest connection and there might, but for the factor of location of storage, be an indeterminate situation.

Illustration:

179. P and Q, located in different states, both engage in the processing of particular data. P and Q have concluded an agreement concerning mutual support, data security standards to be used for data transfers between them, and similar issues. The agreement does not include a choice-of-law clause. In the event of a dispute between P and Q as to their contractual obligations, the forum court must decide which state's law is applicable to the standards for interpreting the agreement. If the other connecting factors are in equipoise, a court can take into account, as a factor in making its choice-of-law decision, the fact that the data is primarily stored on P's servers in P's home state.

Similarly, in a state that requires some sort of connection between the state whose law is selected and the contract at hand or the contracting parties, the fact that data that is the subject of a contract is stored on servers in the designated state can be a factor in the court's determination of whether the required relationship to the designated state is present.

d. Extraterritorial application of law. A state frequently must decide whether, and the extent to which, its laws apply to matters that occur, or are located, outside the borders of that state. Given that in cases involving data the relevant data is very often stored on servers located outside the territory of the state in which all or most of the other elements of the case are located, the application of that state's law is often accused of having undue "extraterritorial" effect. It should be noted, however, that the territorial location of data storage outside a state will typically not raise issues of extraterritorial application of the laws of that state.

Illustration:

180. A court in France issues a judgment according to which car manufacturer M based in France must grant access to particular data to engine manufacturer E based in

Germany. In doing so, the court applied French law, while the data is stored on cloud servers located in the United States. The fact that the French court applied French law despite the fact that the data is stored outside France does not constitute extraterritorial application of French law.

REPORTERS' NOTES

United States:

The relevance of the data storage location is underscored by a U.S. program created in the aftermath of the 9/11 attacks to track and review transactions transmitted by individuals suspected to have ties to Al Qaeda through the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which operated redundant data centers in the United States and the Netherlands. Public disclosure of this program in 2006 led to concerns about whether U.S. authorities' ability to access European banking data violated European law. The United States and the European Union negotiated an agreement to store European data exclusively in the Netherlands effective on August 1, 2020. U.S. Dep't of the Treasury, Terrorist Finance Tracking Program (TFTP), http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx.

The issues are also presented clearly by the high-profile dispute over whether a warrant obtained by the federal government under the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712, required Microsoft Corporation to produce email stored in Ireland. The trial court held that the location of the requested data is irrelevant so long as the party subject to the warrant has control over the requested material, and that requiring production of data stored abroad would not constitute impermissible extraterritorial application of U.S. law. In re Warrant to Search a Certain E-mail Acct. Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014). The Second Circuit rejected all of those legal conclusions on appeal, holding that the statute lacked a clear signal that Congress intended the statute to apply extraterritorially, and that requiring production of the email would be outside the SCA's focus on protecting users' privacy interest in stored communications. In re Warrant to Search a Certain E-mail Acct. Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016). The U.S. Supreme Court granted certiorari and heard oral argument on the case before it was mooted by the enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD) Act, Pub. L. No. 115–141, Div. V, Mar. 23, 2018, 132 Stat. 1213, codified at 18 USC §§ 2713 and 2523, which expedited procedures for international localization of U.S. search warrants. United States v. Microsoft, 138 S. Ct. 1186 (2018). Although that case turned more on the substantive provisions of the SCA than on choice of law, it provides an apt illustration of the issues that can arise and the considerations that are at play.

Although Restatement of the Law Second, Conflict of Laws § 6 lays out the general factors relevant to the choice of applicable law, §§ 188 and 244 of that Restatement recognize that those factors vary somewhat in importance with respect to contracts and property, respectively. Restatement of the Law Second, Conflict of Laws §§ 6, 188, 244 (AM. L. INST. 1971). Both provide that, in the absence of more specific governing provisions, courts should apply the law of the state

that has the most significant relationship to the subject matter and the parties, and list the current location of the subject matter as only one of several considerations that courts should take into account. Id. §§ 188 and 244.

In terms of substantive law, the scope of U.S. federal statutes such as the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA), turns on the nature of the entity, not the location of the data. U.S. state privacy statutes typically apply to the data regarding residents of that state regardless of where the data is stored. See, e.g., CAL. CIV. CODE § 1798.140(g).

Regarding choice of law, some courts have included the location of computer servers as one of the considerations justifying the application of a particular state's law to a dispute. In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 486 (D. Minn. 2015).

Europe:

As data can be moved across the globe within fractions of a second, these Principles limit the relevance of the storage location of data for choice-of-law-purposes. Again, it is of utmost importance to stress that these Principles primarily address situations in which the forum takes a "connecting factor approach" to resolving a potential conflict of laws, and do not give any guidance as to how to define territorial scope, see the Reporters' Notes to Principle 38, Comment *a*. This also means that this Principle does not deal directly with the many instances in which a conflict is resolved by rules defining the territorial scope of a regulatory regime, even though the spirit of this Principle, i.e., that the location of data storage should normally not count, or count only in exceptional cases, will also be relevant when it comes to the territorial scope of regulatory regimes.

When data is the subject of contractual agreement, territorial location of data is irrelevant under existing EU Law. Article 4(2) of the Rome I Regulation (Regulation (EC) No 593/2008) establishes the general rule that, in the absence of an agreement, a contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has its habitual residence. This is also true for sales and service contracts, which are specifically mentioned in Article 4(1)(a)(b) (for more detailed elaborations, see the Reporters' Notes to Principle 38). The location of the subject of the contract is only relevant if a contract relates to a right in rem in immovable property or to a tenancy of immovable property.

Whether the storage location of data is irrelevant, when damage or loss of data results from a tortious act, is still unclear. According to Article 4(1) of the Rome II Regulation (Regulation (EC) No 593/2008), the applicable law to non-contractual obligations arising out of a tort/delict is the law of the country where the damage occurs. Prima facie, that would indicate that the server location of the damaged data determines the applicable law. However, the Court of Justice of the European Union (CJEU) decision *Wintersteiger* (Case C-523/10, ECLI:EU:C:2012:220) can be used as an argument that the server location should not be considered a relevant factor for determining the applicable law. The subject matter of the decision was the jurisdiction in the case of a trademark infringement on the internet through the use of a keyword identical to the protected trademark on a search engine. According to Article 7(2) of Brussels Ia Regulation (Regulation 1215/2012), the defendant may be sued both at the place where the damage occurred and the place of the event giving rise to it. Regarding the latter, the CJEU stated that the technical display process

by the advertiser is activated, ultimately, on a server belonging to the operator of the search engine. However, in view of the objective of foreseeability, which the rules on jurisdiction must pursue, the place of establishment of that server cannot, by reason of its uncertain location, be considered to be the place where the event giving rise to the damage occurred. Some authors argue that this approach should also apply to the Rome II Regulation, and suggest that cases in which data is damaged or lost should be solved by applying the "closest connection" rule of Article 4(3) of the Rome II Regulation (see Carl Friedrich Nordmeier, Cloud Computing und Internationales Privatrecht, (2010) *MultiMedia und Recht*, p. 151, 154; Georg Haibach, Cloud Computing and European Union Private International Law, (2015) *Journal of Private International Law*, 252, 264ff).

Currently, no ownership-like rights for data exist in the European Union, not even in European legal systems that adhere to the "broad notion of legal object." Hence, the application of the *lex rei sitae* to data rights is not decisive, and the storage location does not play a role for the applicable law. In addition, referring to a single applicable legal system—as the *lex rei sitae* does for property rights—would not be appropriate for data rights, as they are not exclusive rights, but rights that take into account the special characteristic of data as a non-rivalrous good. It has been suggested that the regime of the General Data Protection Regulation (GDPR) be followed (Article 3 and Recital 153 GDPR; see the Reporters' Notes to Principle 38) for data rights that have no connection to a contractual relationship. An entity should be able to rely on a data right existing in a country if the data processing in question is carried out as part of the activities of an establishment of the respondent in that country. Whether the processing takes place in that country or the data are collected and processed in the context of an activity directed toward that country should be considered irrelevant (see Christiane Wendehorst, in Jürgen Säcker/Roland Rixecker/Hartmut Oetker/Bettina Limperg, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 13 – Internationales Privatrecht, 2020, Art. 43 EGBGB para 296 ff).