

ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights –

GUIDE TO THE PRINCIPLES

for the webinar on 5 December 2023

Note:

This Guide is intended to facilitate access to the
ALI-ELI Principles for a Data Economy.

Authors:

Steven O. Weise, Proskauer Rose LLP, Bainbridge Island, WA, U.S.A.
ALI Chair of the ALI-ELI Principles for a Data Economy

John Thomas, Lord Thomas of Cwmgiedd, Essex Court Chambers, formerly Lord Chief Justice of England and Wales, The United Kingdom
ELI Chair of the ALI-ELI Principles for a Data Economy

Neil B. Cohen, Brooklyn Law School, Brooklyn, NY, U.S.A.
ALI Reporter of the ALI-ELI Principles for a Data Economy

Christiane C. Wendehorst, Professor of Law at the University of Vienna, Austria,
ELI Reporter of the ALI-ELI Principles for a Data Economy

Yannic Duller, University of Vienna, Austria, Yannic.duller@univie.ac.at
ELI Consultant of the ALI-ELI Principles for a Data Economy

Sebastian Schwamberger, University of Vienna, Austria, Sebastian.schwamberger@univie.ac.at
ELI Consultant of the ALI-ELI Principles for a Data Economy

TABLE OF CONTENT

1. INTRODUCTION	4
2. ABOUT THE PROJECT	5
2.1. General Aim and Approach	5
2.2. Players and Relations in the Data Ecosystem.....	5
2.3. Structure of the Principles.....	7
3. DATA CONTRACTS (PRINCIPLES 5 TO 15)	7
3.1. Contracts for supply or sharing of data (Principles 7 to 11).....	8
3.2. Contracts for services with regard to data (Principles 12 to 15).....	9
4. DATA RIGHTS (PRINCIPLES 16 TO 27).....	10
4.1. Four Data Rights.....	10
4.2. The differentiation between two types of data rights	10
4.3. Data Rights with regard to Co-Generated Data (Principles 18 to 23).....	11
4.3.1. Factors to determine co-generation	11
4.3.2. Factors to be considered when granting a data right	11
4.3.3. Legitimate grounds for specific types of data rights	12
4.4. Data Rights for the Public Interest and Similar Interests (Principles 24 to 27)	13
5. THIRD PARTY ASPECTS OF DATA ACTIVITIES (PRINCIPLES 28 – 37)	15
5.1. Wrongfulness of Data Activities vis-à-vis Third Parties (Principles 28 – 31).....	15
5.2. Effects of Onward Supply on the Protection of Others (Principles 32 – 34).....	15
5.3. Effects of Other Data Activities on the Protection of Third Parties (Principles 35 – 37)	17

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



1. Introduction

The Authors were significant participants in the preparation of the “ALI-ELI Principles for a Data Economy” (“the Principles”), a project jointly conducted by the European Law Institute (ELI)¹ and the American Law Institute (ALI)².

The Principles aim at developing a cross-sectoral governance framework in the form of transnational Principles that can be used as a source for inspiration and guidance for legislators and courts worldwide. They can further inspire the development of codes of conduct and sector-specific standards as well as facilitate the drafting of model agreements or provisions to be used on a voluntary basis by parties in the data economy. The Principles have already gained international attention in the field of data governance.

In 2019, the approach on co-generated data set out in the Principles was adopted in its entirety by the German Data Ethics Commission in its final report.³ Furthermore, the OECD's Global Partnership on AI (GPAI) has largely based its work on data rights and transactions on the preparatory findings in the Principles.⁴ Finally, the Principles heavily impacted recent work by and deliberations at meetings of Working Group IV on Electronic Commerce at UNCITRAL. The Principles are listed as one of the essential and most innovative sources in the field of data transactions and data rights.⁵ The Reporters of the Principles are also in close contact with scholars working on the legal challenges posed by the data economy from across the world including from Japan and China.

In addition, the project team has always sought to be actively involved in legislative processes in the area of data rights and data transactions. From a European perspective, the procedure leading up to the adoption of the Data Act⁶ is particularly significant. The project team submitted a statement in response to the public consultation⁷ and was actively engaged in the exchange with members of the European Commission at various conferences and meetings. This ultimately led to the approach to data rights on co-generated data developed in the Principles being reflected in the Data Act⁸.

¹ <<https://europeanlawinstitute.eu/principles-for-a-data-economy/>>.

² < <https://www.ali.org/publications/show/data-economy/>>.

³ Opinion of the Data Ethics Commission, 2019, p. 85 ff., available via <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html>.

⁴ GPAI, Data Governance Framework, 2020, available via <https://gpai.ai/projects/data-governance/gpai-data-governance-work-framework-paper.pdf>.

⁵ UNCITRAL, A/CN.9/1117 - Legal issues related to digital economy – proposal for future work on data transactions, available via <https://uncitral.un.org/en/commission>.

⁶ The Data Act has been recently adopted by the European Legislator and will soon be published in the Official Journal. The Data Act in the version adopted by the Council of the European Union on 27 November (2022/0047 (COD)), available via <https://data.consilium.europa.eu/doc/document/PE-49-2023-INIT/en/pdf>.

⁷ See Christiane Wendehorst, Lord John Thomas and Sebastian Schwamberger, Response to the Public Consultation on “A European Strategy for Data” COM(2020) 66 final, available via <https://bit.ly/2NvtncU>.

⁸ See in particular Article 3 and 4 Data Act.

2. About the Project

2.1. General Aim and Approach

The ALI-ELI Principles for a Data Economy aim to address the existing legal uncertainty when it comes to data transactions and data rights. The application of traditional legal doctrines to trade 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. 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. 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 utilise 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.

The fact that data is different to other commodities in so many ways is the reason that it has become necessary to draft a specific set of principles for data transactions and data rights instead of merely referring to the existing law of, say, sale and lease of goods, or of property. 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). The ALI-ELI Principles for a Data Economy provide a set of principles that can be implemented in any kind of legal environment, and 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.

2.2. Players and Relations in the Data Ecosystem

The Principles cannot provide a complete set of standards for any sort of dealings within the data economy. They have taken the following (simplified) model of a data ecosystem as a starting point:

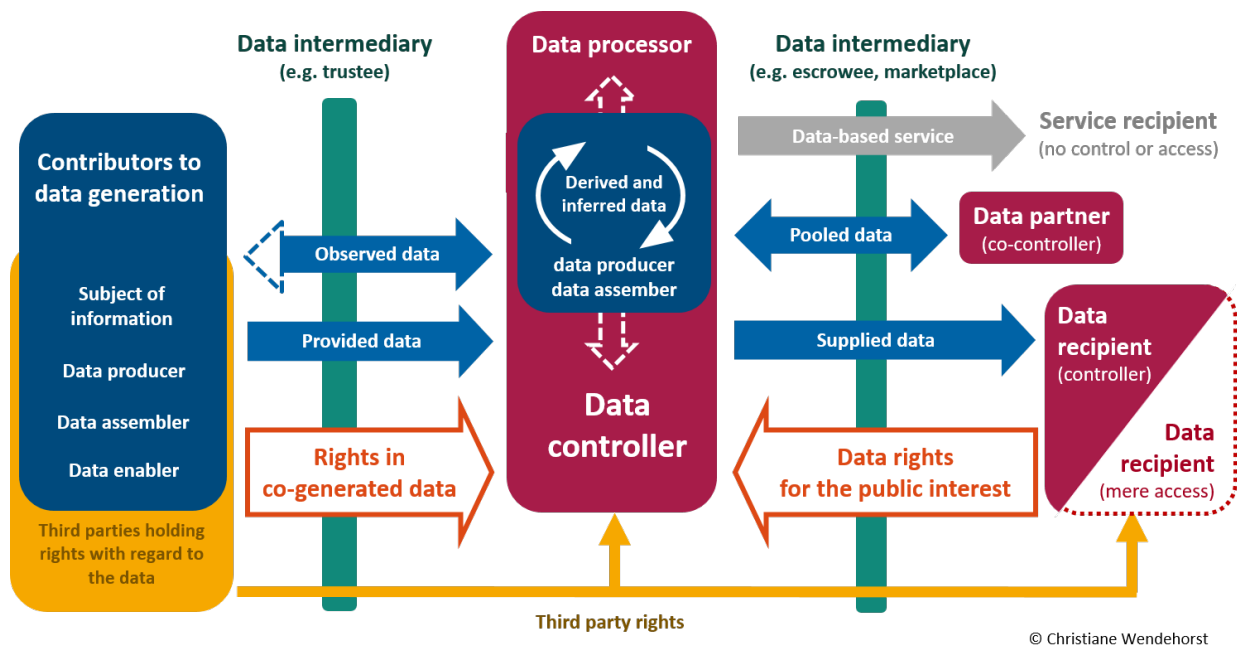


Figure 1: Players in the data ecosystem (simplified)

The central player 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 its processing. A (mere) processor of data, on the other hand, is a service provider that processes data on a controller’s behalf. 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 where data is fully transferred to them, or they may receive only access to the data, such as where they are permitted to process data with a mobile software agent on the supplier’s server.

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 contribute in other roles. Often, parties contributing to the generation of data have third party rights with regard to the data, such as rights arising from data protection law, intellectual property law, or from contractual restrictions, but the parties contributing to the generation of data and the parties holding third party rights do not always fully coincide.

In addition to the parties mentioned, there is 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 trusted third party.

The players mentioned may enter into contractual arrangements with regard to data. However, with or without the existence of a contractual relationship, particular parties may have certain rights with regard to the data, which are normally exercised vis-à-vis the controller of data. Such data rights may have their

justification in a share which the party relying on the right had in the generation of the data (rights in ‘co-generated data’) or in the public interest.

2.3. Structure of the Principles

The Principles are divided into five Parts. After general provisions (Principles 1 to 4), which set out the purpose, scope and definitions, Part II (Principles 5 to 15) identifies several different categories of data contracts and provides default rules for each of them. Part III is dedicated to data rights, such as data access rights, be it with regard to data that has been co-generated by the party exercising the data right or with regard to other data. The fourth Part (Principles 28 to 37) deals with third party aspects of data activities, which is especially important when data is personal data or is protected by, for instance, intellectual property law or by contractual restrictions on data utilisation. The Principles close with Part V (Principles 38 to 40) which is on multi-state Issues.

The following figure shows how the different Parts and Chapters of the Principles address the relationships between the various players in a data ecosystem:

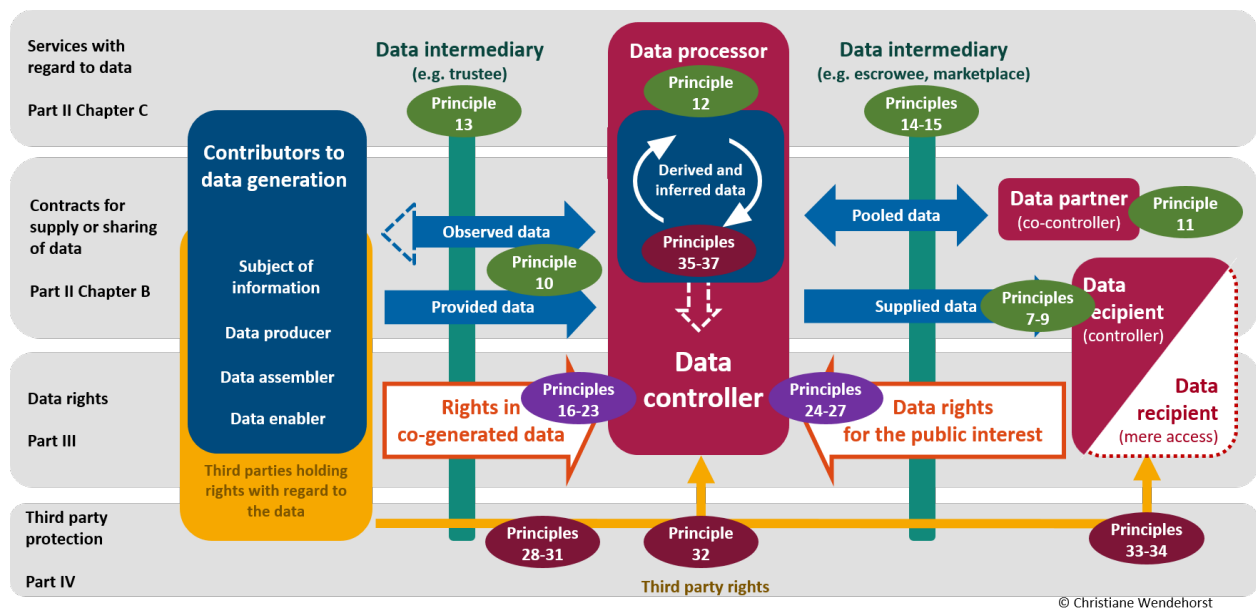


Figure 2: Players in the data ecosystem and how they are addressed by the Principles

3. Data Contracts (Principles 5 to 15)

Data has become an economic resource, traded like traditional assets and commodities under contractual agreements. However, existing contract law does not currently take into account the special characteristics of data and consequently is silent on many core issues that may arise in negotiating data transactions or in disputes with respect to them. For example, is the recipient of data supplied under a contract entitled to

utilise received data for any (other) lawful purpose or only for the purposes expressly stated in the contract (i.e., sales vs licence approach)? May a party providing services with regard to the data also use the data for its own purposes? The lack of default provisions in current law specifically tailored for data transactions not only adds costs in negotiation and creates transactional uncertainty for parties that want to engage in data transactions, but the lack of such provisions also makes decisions more difficult for courts and arbitral tribunals that are dealing with incomplete agreements. It is especially for such scenarios that Part II of the Principles sets out default rules for two categories of data contracts: (i) contracts for supply and sharing of data (Chapter B, Principles 7 to 11), and (ii) contracts for services with regard to data (Chapter C, Principles 12 to 15).

3.1. Contracts for supply or sharing of data (Principles 7 to 11)

Chapter B sets out default rules for five types of contracts for the supply and sharing of data:



**Contracts for
the transfer of
data**

In a **data transfer** contract under Principle 7, the supplier undertakes to put the data recipient in control of particular data (e.g. by transferring the data to a medium within the recipient's control). By default, a 'sales approach' is suggested, i.e. the recipient, is entitled to use the data for any lawful purpose that does not infringe the rights of the supplier or third parties.



**Contracts for
simple access to
data**

Where parties do not wish to provide full control of the data to the recipient, they could choose a contract for **simple access to data** within the meaning of Principle 8. This contract type allows the recipient to access particular data on a medium within the supplier's control. By default, the recipient may utilize the data only for the purposes agreed or required by law ('license approach').



**Contracts for
exploitation of a
data source**

A contract for exploitation of a data source within the meaning of Principle 9 is one under which the supplier undertakes to provide to the recipient access to a **data source**, i.e. a device or facility by which data is collected or generated. The recipient can view, process or port data from the data source, usually in real-time.



Contracts for authorization to access

On the basis of contracts for **authorization to access** under Principle 10, the supplier authorizes the access to data by the recipient, but takes on a much more passive role and usually does not undertake any obligations regarding the data (e.g. consumers using ‘free’ services and supplying user data in return).



Contracts for data pooling

In a **data pooling** arrangement within the meaning of Principle 11, two or more parties ('data partners') share data by transferring it to a jointly controlled medium, or in other ways. This requires default rules as to mutual rights and obligations, including on derived data, sharing of profits, and on the situation when a partner leaves the data pool.

3.2. Contracts for services with regard to data (Principles 12 to 15)

Part II Chapter C deals with four types of contracts whose focus is not the supply of data by one party to another, or the sharing of data among various parties, but rather the performance of services with regard to data.



Contracts for the processing of data

Principle 12 covers contracts in which a processor undertakes to **process data** on behalf of the controller. Examples are data scraping, data analysis and data storage as well as data management services. The processor must follow the controller’s directions and act consistently with any stated purposes, may normally not use the data for its own purposes, and must transfer the data to the controller, or a third party designated by the controller, at the controller’s request.



Data trust contracts

Principle 13 sets out default rules for typical **data trust arrangements** (which should not be taken as encompassing the specific implications of the common law concept of trusts), with the trustee acting as intermediary between suppliers of data and data recipients.



Data escrowee contracts

In order to comply with legal requirements (imposed, e.g., by applicable data protection law or antitrust law), parties engaging in data activities may want to limit their powers over the data by transferring certain powers and abilities to a trusted third party (the escrowee) under a **data escrow contract** within the meaning of Principle 14.



Data marketplace contracts

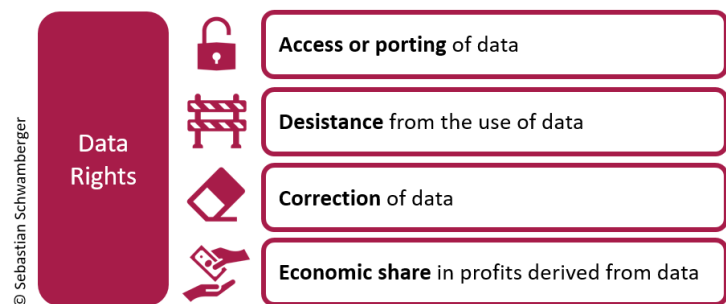
A data marketplace services provider fulfils a matchmaking function between suppliers and recipients of data but may also provide additional services that facilitate the transaction. Both the contract between sup-

plier and platform as well as for the contract between recipient and platform are considered **data marketplace contracts** within the meaning of Principle 15.

4. Data Rights (Principles 16 to 27)

4.1. Four Data Rights

‘Data rights’ are rights against a controller of data that are specific to the nature of data and that arise from the way in which data is generated, or from the law for reasons of public interest. In Principle 16, a non-exclusive list of four types of data rights is identified. The most important type in the data economy is the



right to access data controlled by another party. The meaning of ‘access’ is broad and can cover the mere possibility to read data as well as the ability to engage in varying degrees of processing the data on a medium in the controller’s sphere up to full portability of the data. The Principles consider the different degrees of ‘access’ as part of the modalities of how access is granted.

Another data right of practical importance is the right to require desistance from particular data activities, which can go as far as to include the right to require the erasure of data. A related data right is the right to require correction of incorrect or incomplete data. Finally, under exceptional circumstances, parties may have a right to require an economic share in profits derived from the use of data.





4.2. The differentiation between two types of data rights

Part III of the Principles distinguishes between data rights that are afforded to parties that had a share in the generation of the relevant data (Principles 18 to 23) and data rights afforded to persons that did not have a share in the generation of the data but that should nevertheless have a data right for other overriding considerations of a more public law nature (Principles 24 to 27). Data rights with regard to co-generated data follow a private law logic and are justified by the fact that the party that is afforded a data right had a share in the generation of the relevant data. Data rights with regard to co-generated data fulfil 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 the Principles, as the Principles focus on the nature of the rights and not on their doctrinal classification. Unlike intellectual property rights, rights in co-generated data do not afford their holder a clearly defined range of rights with erga omnes-effect, but rather data rights are of a more flexible nature and depend very much on the parties involved, and on a number of factors in the particular situation.

4.3. Data Rights with regard to Co-Generated Data (Principles 18 to 23)

4.3.1. Factors to determine co-generation

Since the share which a party had in the generation of the data is the justification for introducing a right in co-generated data, Principle 18 lists four factors to determine whether and to what extent data is to be treated as being co-generated by a particular party:

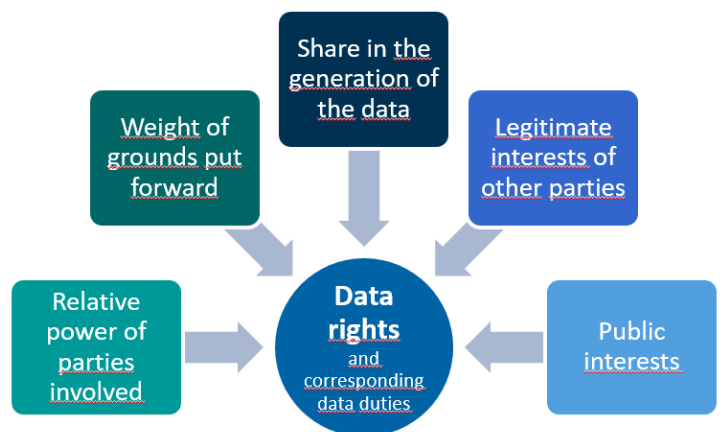
- © Sebastian Schwamberger
-  The extent to which that party is the subject of the information coded in the data, or is the owner or operator of an asset that is the subject of that information;
 -  The extent to which the data was produced by an activity of that party, or by use of a product or service owned or operated by that party;
 -  The extent to which the data was collected or assembled by that party in a way that creates something of a new quality; and
 -  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.

The factors in Principle 18 partly reflect considerations of personality rights, partly they reflect the “labor theory of property” and partly they 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.

4.3.2. Factors to be considered when granting a data right

The share which a particular party had in the generation of the data cannot alone be a sufficient justification for granting a right in the data, such as an access right. Rather, there should be a careful balancing of all interests involved. The Principles identify five general factors to be considered when granting a data right:

- (1) The share a party had in generating the data,
- (2) the weight of grounds put forward by the party seeking a data right;
- (3) the weight of any legitimate interests the controller or a third party may have in denying the data right;
- (4) any imbalance of bargaining power; and
- (5) any public interest including the interest to ensure fair and effective competition.



© Christiane Wendehorst

The effects of a data right are to a large extent determined by the modalities with regard to formats, timing and the like, and by whether access must be provided for free or in return for appropriate remuneration. The factors put forward by the Principles are not only intended to provide a basis for deciding on whether or not to grant a data right with regard to co-generated data, but also for determining the modalities of how this right should be granted.

4.3.3. Legitimate grounds for specific types of data rights

The grounds that can be put forward by the party seeking to establish a data right, as well as the controller's or third parties' legitimate interests in denying it, are spelt out in more detail in Principles 20–23, addressing specific grounds for the four types of data rights that should be taken into account together with the general factors to be considered when granting a data right.

Illustration 1:

Business T produces tires that are supplied to car manufacturer C and mounted on cars that are ultimately to be sold to end users such as E. Data concerning the tires is generated in the course of mounting of the tires by C (e.g. the robot mounting the tires tests the properties of the rubber) and in the course of E driving the car (e.g. the car sensors collect data on how well tires adapt to weather conditions and road surfaces and how quickly the tires' treads wear off). T seeks access to the data concerning its tires, as it would enable T to improve tire performance. However, C declines to grant such access because C considers producing tires itself at some point and wants to have a competitive edge over T.

The data concerning the tires is considered to have been co-generated to different extents by T, C and E. Quality monitoring and improving its own services are strong legitimate grounds for a supplier in a value chain to claim access to co-generated data. However, the legitimate interests of the controller and third parties (such as E) as well as the relative bargaining power and public interests (e.g. a fair and competitive market) have to be taken into account when affording a data right. While not much weight needs to be given to the interest C to forestall competition, it needs to be ensured that E's rights under the GDPR are not undermined. In order to protect E's privacy a data right vis-à-vis D should be afforded only with appropriate restrictions, such as anonymisation or access via a trusted third party. The costs of these safeguards need to be borne by the beneficiary T.

Illustration 2:

Farm corporation F buys a 'smart' tractor which has been manufactured by manufacturer M and which provides various precision farming services, including weather forecasts and soil analyses. M also uses the soil and weather data collected by the tractor to create a database that can be accessed by potential buyers of farmland, providing extensive details about the land in order to enable them to make a more-informed choice on the price they would be willing to pay for farmland. When F learns about this database, F immediately requests M to stop using F's data for this purpose.

While the party contributing to the generation of data will often have an interest to access or port data, there may be situations where other data rights, such as the right to require a controller of co-generated

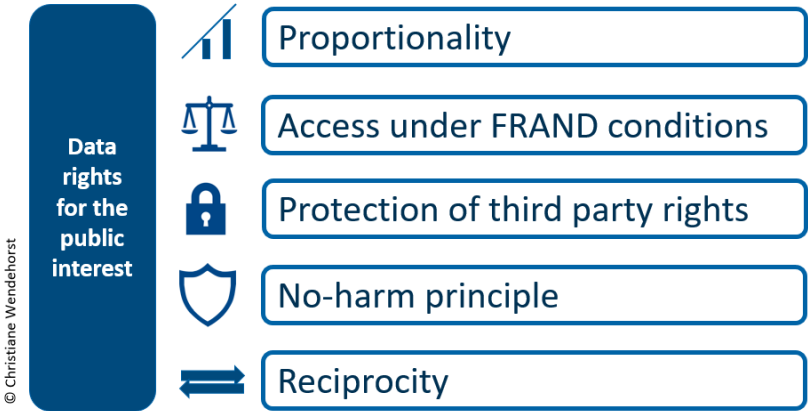
data to desist from particular data uses, are necessary to achieve the desired outcome. According to Principle 21, the fact that the data use is likely to cause significant harm to F is a strong indicator that affording a right to require desistance is justified. However, that alone is normally not sufficient. Additionally, F must have contributed to the generation of the data for another purpose that is inconsistent with the contested use, and could not reasonably have been expected to contribute to the generation of the data if it had foreseen the resulting harm.

Principle 22 deals with the grounds a party has to put forward to be afforded a right to require correction of co-generated data that is incorrect. Since improving the quality of data is in the general interest of the data economy, the threshold is much lower than for requiring desistance.

It has been a major point of controversy both in the U.S. and in Europe whether parties should ordinarily have a right to receive an economic share in the profits derived from the use of co-generated data. The Principles do not take any position as to the general desirability of any particular regime for the distribution of wealth among the different players in the data economy, and as to whether policymakers should seek to achieve it. However, the grounds suggested by Principle 23 which a party may rely on to have an enforceable data right, beyond contractual rights and rights following from other bodies of the law (such as the law of unjust enrichment), to receive an economic share in the profits derived from co-generated data are very narrow. Only if a party's contribution is particularly unique or based on an extraordinary investment and further requirements are met, such a right should, according to Principle 23, be granted.

4.4. Data Rights for the Public Interest and Similar Interests (Principles 24 to 27)

While data rights with regard to co-generated are based on the share a party had in the generation of the data, data rights may also be justified if the interests of the controller are outweighed by legitimate public interests or similar overriding considerations. Principles 24 to 27 give concrete guidance for legislators on the introduction of data rights for the



public interest by setting out five basic values: (1) proportionality; (2) access under fair, reasonable and non-discriminatory conditions (FRAND) conditions; (3) protection of third party rights; (4) no-harm principle; and (5) reciprocity. These Principles could also be used to supplement legislation that is silent on certain points, or where the respective point is left to negotiations between the controller and the recipient.

First and foremost, data rights should not only be justified by a public interest but also necessary and proportionate to achieve the pursued objective (Principle 24). Quite regularly, the public interest that justifies

the creation of a data right will be the prevention of a market failure, which would lead to higher prices, lower quality of services, less innovation, and less choice for consumers. Thus, data rights for the public interest overlap with competition law. However, it has already been stressed in several studies that competition law is too slow to address urgent competitive concerns since proceedings can last for several years. Furthermore, there are various other public interest considerations that can justify data rights. For example, the access right under the European REACH Regulation seeks to avoid unnecessary duplication of tests that have a significant impact on our environment and cause unnecessary harm to animals.⁹

Secondly, the law should provide that data rights for the public interest are granted on fair, reasonable and non-discriminatory conditions (Principle 25(1)). Where affording a right would be in conflict with protected rights of third parties or competing public interests, a policymaker should ensure that appropriate restrictions such as disclosure only to a trusted third party, disaggregation, anonymisation or blurring of data, are in place (Principle 25(2)).

Data rights established for the public interest could grant the recipient the right to use the data exclusively for the purposes for which the right had originally been afforded, or also allow usage for other purposes. The Principles recommend the latter approach, stating that the recipient may use the data in any lawful way and for any lawful purpose as long as this is consistent with a number of limitations. Most notably the data may not be used for a purpose that contravenes or undermines the public interest. It is, however, not enough that the type of data use simply failed to be contemplated by the legislator when the access right was created (Principle 26(1)) Furthermore, the data may not be used in way that it harms the legitimate interests of the original controller more than is inherent in the purpose for which the right was afforded. As the innovative use envisaged by B in illustration 6 is not explicitly excluded by the relevant statute, and is neither inconsistent with the original purpose nor harms M, B should be allowed to use the data for this purpose.

Illustration 3:

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.

From general considerations of fairness, it follows that the party receiving data under a data sharing regime for the public interest, should normally be prepared to share similar data under similar conditions with the controller that had originally shared the data (Principle 27). However, whether such a reciprocal data right should be afforded ultimately depends on the concrete public interest. For example, where SMEs are

⁹ Recital 40, Regulation (EC) No 1907/2006.

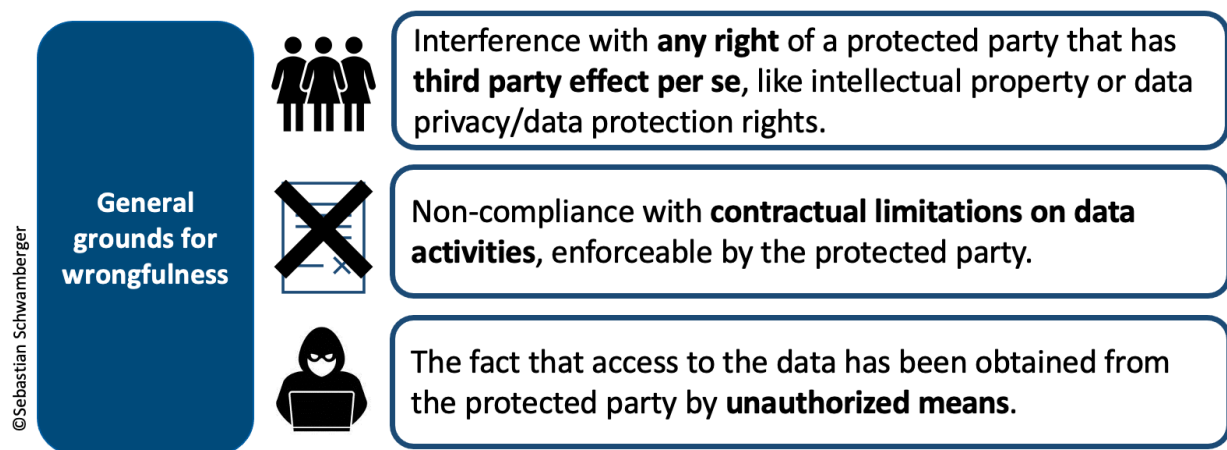
granted access right is vis-à-vis dominant market players, introducing a similar right to the latter would frustrate the pursued objective of ensuring effective competition.

5. Third Party Aspects of Data Activities (Principles 28 – 37)

Data contracts as well as data rights will regularly not only produce effects between the contracting parties or between the party exercising a data right and the party against whom the right is exercised, but will also affect the legitimate interests of third parties.

5.1. Wrongfulness of Data Activities vis-à-vis Third Parties (Principles 28 – 31)

Principle 28 sets out a non-exhaustive list of cases where a data activity is considered to be wrongful:

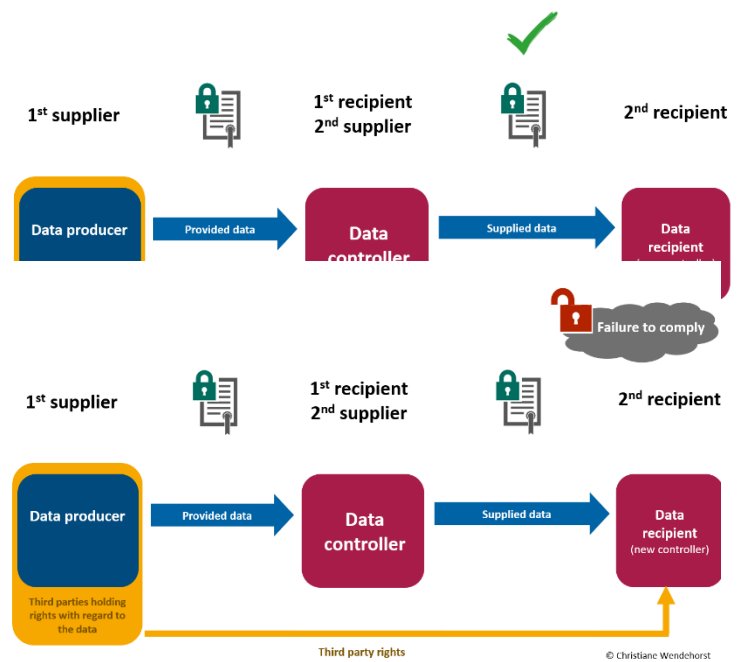


5.2. Effects of Onward Supply on the Protection of Others (Principles 32 – 34)

Resolving the more difficult question of whether and to what extent the wrongfulness of a data activity also affects downstream recipients requires careful balancing: Giving third party rights full effect under all circumstances against every recipient down a stream of transactions would overly discourage parties from sharing data or investing in data. However, protection of downstream recipients must also not undermine third party protection. The regime ultimately recommended by the Principles has been inspired in part by trade secrets protection.

Principle 32 addresses this issue by setting out a duty for any supplier to ensure that recipients will comply with the same duties and restrictions as the supplier. Hence, the supplier, as well as any recipient, who in turn makes data available to further downstream recipients, is obliged to pass on restrictions and duties. Additional safeguards (such as penalties or technical limitations) might be necessary depending on the potential risk for protected parties.

If a downstream recipient infringes protected interests of third parties by engaging in wrongful data activities, the supplier will not be liable vis-à-vis the initial supplier if it can prove it has complied with its duty under Principle 32. However, Principle 33 affords the initial supplier the right to take direct action against downstream recipients after notice has been given to the immediate recipient.



In addition to the grounds of wrongfulness that take direct effect vis-à-vis a downstream recipient (e.g. under applicable data protection law) Principle 34 provides that the data activities of a downstream recipient are wrongful if that recipient had notice or ought to have notice that the supplier acted wrongfully. Without Principle 34, contractual obligations, such as the restriction on the downstream supply, would only produce effect between the contracting parties and might leave the initial supplier without protection. Principle 34 also strengthens the position of the initial controller if the data is ‘stolen’ and then passed on to a recipient who had notice (or ought to have notice) of the wrongful activities of the data thief, as it allows the initial controller to take action against both the thief and the recipient.

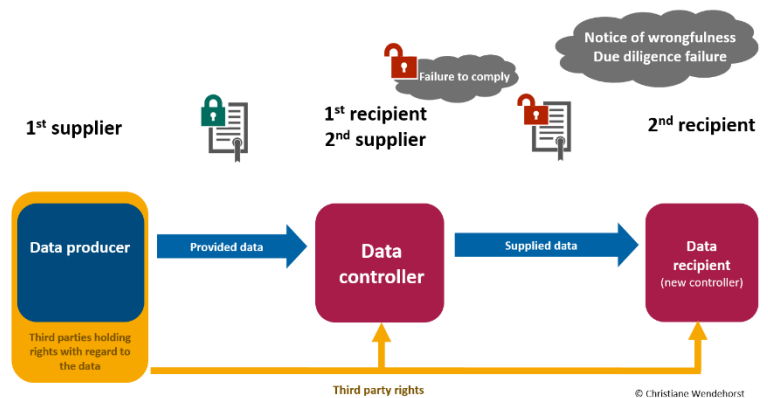


Illustration 4:

M manufactures smart tractors, “sells” the data generated by the fleet of its tractors to fertiliser producer F, who wants to use the data to improve the efficiency of the fertilisers on certain soils. The contract between M and F entitles F to sell the data to third parties but limits the use of the data to the purpose of improving fertilisers. However, when F “resells” the data to another fertiliser manufacturer T, no purpose limitation clause is included in the contract between F and T. Consequently, T uses the data not

only to improve its products, but also to develop software that recommends smart tractor users appropriate fertilisers for their soil.

Principle 32 requires F to impose the same restrictions regarding data use on downstream recipient T. Since F failed to contractually limit T's data use to improving the efficiency of fertilizers, F's data activity (the onward transfer) is wrongful. Whether the data activities of T (using the data to develop software) are also wrongful is determined by Principle 34. If T, at the time the data activity was conducted, had notice that F is acting wrongfully or failed to make such investigation as could reasonably be expected under the circumstances, T's data activities are wrongful.

5.3. Effects of Other Data Activities on the Protection of Third Parties (Principles 35 – 37)

Quite regularly, a downstream recipient of data will aggregate the received data with other data and/or process it in order to obtain new data from it. Whether and to what extent the obligations and limitations for the original data set also apply to derived data generally depends on the specific regime governing the protected right. For example, if personal data is altered in a way that it no longer relates to an identified or identifiable natural person, data protection law does not apply to the derived anonymised data.¹⁰ Where the applicable regime is either silent or only allows for equivocal conclusions, Principle 35(2) suggests taking into account (i) the degree to which the derived data is different from the original data as well as (ii) the degree to which the derived data poses a risk to a protected party compared to the original data.

If the original data was processed wrongfully, but duties and restrictions do not prevail with regard to the derived data, the unlawful processor could keep and use the derived data without any limitations. Since this result may encourage reckless infringements of a protected right, Principle 36(1) requires a controller that has engaged in wrongful processing activities to disaggregate, reverse-engineer, or delete the derived data, but also recommends a range of exceptions to this rule.

Illustration 5:

Car manufacturer M holds large amounts of traffic data from connected cars. M grants a 'license' to application developer D according to which D may use particular data for developing an app that helps drivers find free parking space, but D may not disclose the data to any third party nor engage in the development of a defined list of activities that might harm M's economic interests. D, in violation of the contractual terms agreed with car manufacturer M, uses the data received from M for inferring certain data about car emissions (with a view to developing an app that would help drivers to cut on emissions). While processing the data for that purpose was clearly wrongful (as in breach of contract), the question arises whether D may keep the derived data on car emissions, production of which has cost D a fortune, and/or the app developed on their basis.

¹⁰ See Article 4(1), Recital 26 GDPR (Regulation (EU) 2016/679)

As a ground rule, Principle 36(1) states that D in Illustration 5 must destroy any data or service derived from a wrongful data activity. However, deleting the derived data and stopping the development of the app would lead to the destruction of value that may be unreasonable in light of the circumstances giving rise to wrongfulness. For these cases, Principle 36(2) provides the possibility to keep the data and make an allowance in money instead. The factors that need to be taken into account are (i) whether D had notice of the wrongfulness, (ii) the purpose of the processing, the amount of investment, and (iii) whether the wrongfulness was material and could cause relevant harm to M. Using data to cut emissions is in the public interest and unlikely to harm M's legitimate interests. Hence, D may be afforded the right to make an allowance in money instead of erasing the wrongfully derived data. The same holds true for the app that is being developed with the help of the derived data (Principle 36(3)).

Since data, which may be subject to a variety of different legal regimes, is to an increasing extent compiled in very large and diverse datasets, it has become extremely difficult for controllers of such datasets to ensure that none of the data violates protected rights. The Principles recognise this and provide for an exception if only a minimal amount of data in a large dataset is in non-compliance with a protective regime. According to Principle 37, a data activity is not wrongful if (i) the non-compliance is not material in the circumstances, (ii) the controller has made reasonable efforts to comply with the duties and restrictions and (iii) the data activities are not related to the purpose protection and could not reasonably be expected to cause material harm to a protected party. This exception only protects the controller from claims that the activity regarding the whole dataset is wrongful. The wrongful data as such still needs to be removed from the large dataset, unless this would be unreasonable in the circumstances.