ALI/ELI Principles for a Data Economy
Data Transactions and Data Rights

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

<u>Principle 11. Contracts for Data Pooling</u>

(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.

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.

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.

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.

<u>Principle 15. Data Marketplace Contracts</u>

(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 whether the matchmaking results in a data transaction.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.