

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

Outline for the international online conference
on 18 and 19 October 2021

Note:

This Outline is intended to facilitate access to the
Final Draft of the ALI-ELI Principles for a Data Economy.

The explanatory text, which has been drafted by the Reporters, Chairs and Consultants of the project is not the original text, and it has not been officially authorised by either the ALI or the ELI. Blackletter Principles in the Annex have been approved by the ALI Council and Membership and by the ELI Council and Membership

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	4
2.1. General Aim and Approach	4
2.2. Players and Relations in the Data Ecosystem.....	5
2.3. Structure of the Principles.....	6
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
ANNEX: BLACKLETTER OF FINAL COUNCIL DRAFT	19

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)^{2,3}. The most recent draft, titled ‘ELI Final Council Draft’, is publicly available⁴ [here](#). It has been approved by the Council and the Membership of the ALI as well as by the Council and Membership of the ELI.

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 particular, its approach on co-generated data in Part III has been adopted by the German Data Ethics Commission,⁵ and the Data Governance Working Group of the Global Partnership on AI (GPAI)⁶. Moreover, the Principles have been recognised by UNCITRAL as one of the main international sources setting out legal rules applicable to data transactions.⁷ UNCITRAL is currently examining the possibility of developing harmonised legislative solution for legal issues related to data transactions.⁸ 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.

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 trades in data is not well-developed, often does not fit the trade, and is not always useful or appropriate or even accomplished in a consistent manner. At the bottom of this uncertainty lies the fact that data is different from other resources in several ways, such as by being what has come to be called a ‘non-rivalrous resource’, i.e. data can be

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

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

³ See also the project homepage: <<https://principlesfordataeconomy.org/>>.

⁴ The draft can be downloaded for free at the ALI Project homepage <<https://www.ali.org/projects/show/data-economy/>>

⁵ Opinion of the German Data Ethics Commission (2019), p. 85 ff., <<https://www.datenethikkommission.de/>>.

⁶ Jančí et al., Data Governance Working Group: A Framework Paper for GPAI’s work on Data Governance (2020).

⁷ A/CN.9/1012/Add.2 paras 6 ff, 15; A/CN.9/1064/Add.2 paras 8 ff.

⁸ United Nations, General Assembly, *Legal issues related to the digital economy – data transactions*, A/CN.9/1012/Add.2, 12 May 2020, available via <<https://undocs.org/en/A/CN.9/1012/Add.2>>; United Nations, General Assembly, *Revised draft legal taxonomy – revised section on data transactions*, A/CN.9/1064/Add.2, 24 May 2021, available via <https://uncitral.un.org/sites/uncitral.un.org/files/1064_add_2_advance_copy_e.pdf>.

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

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:

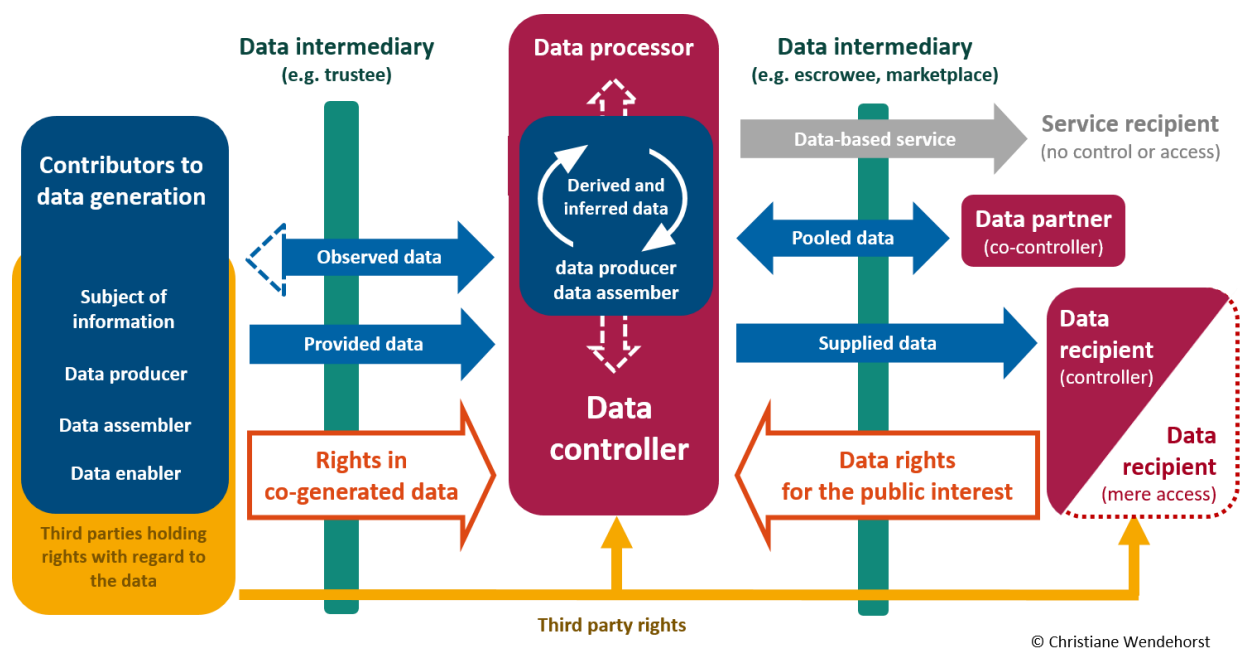


Figure 1: Players in the data ecosystem (simplified)

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 following 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:

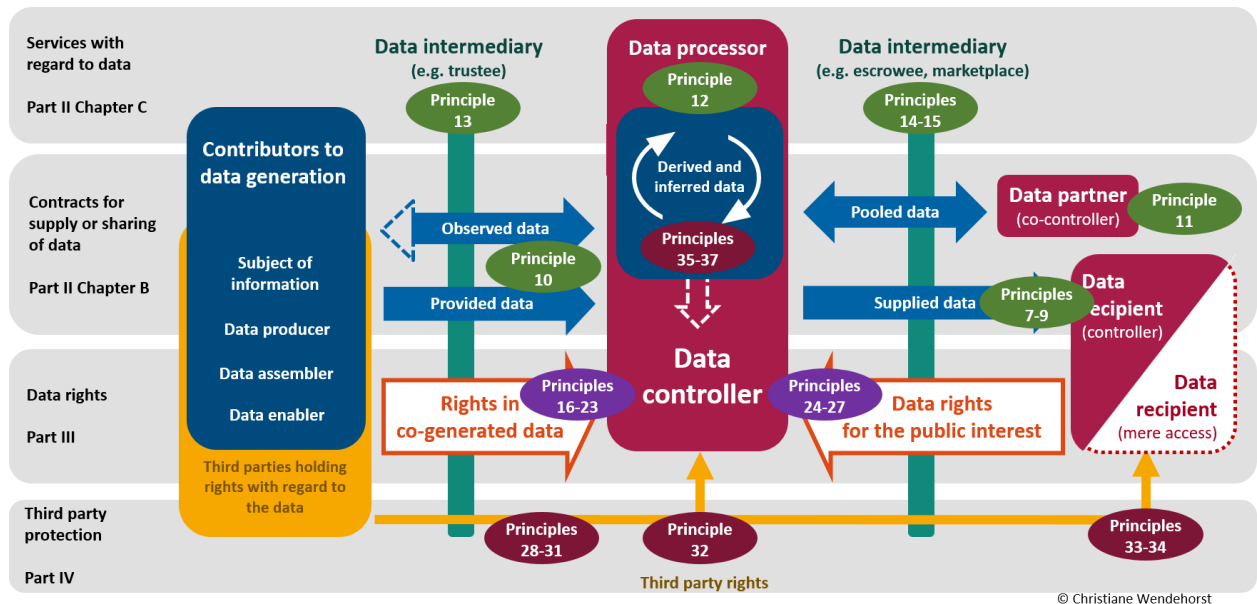


Figure 2: Players in the data ecosystem and how they are addressed by the Principles

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 negotiating data transactions or 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 aim 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.



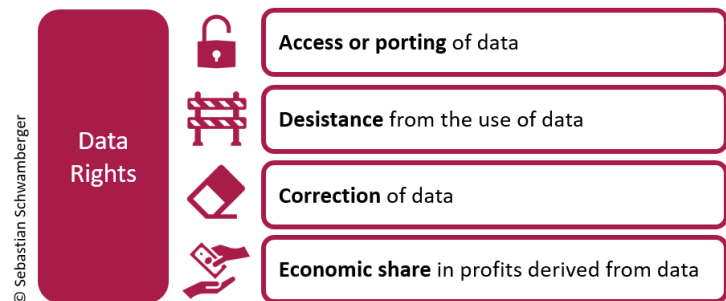
Data marketplace contracts

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 supplier 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:

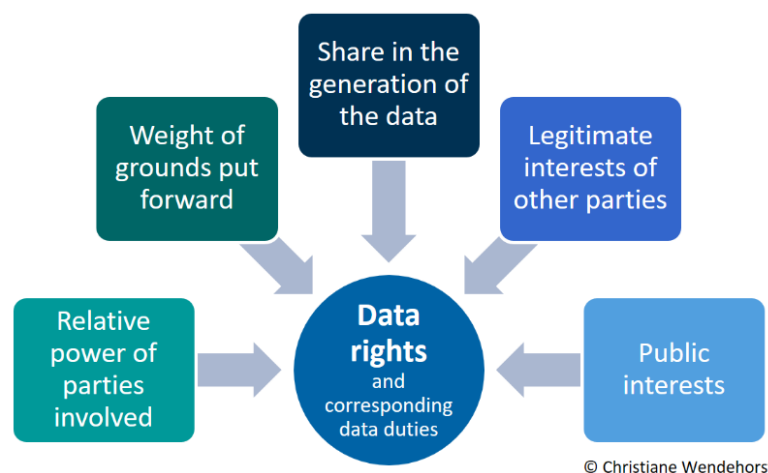
- © Sebastian Schwamberger
-  The extent to which that party is the subject of the information coded in the data, or is the owner or operator of an asset that is the subject of that information;
 -  The extent to which the data was produced by an activity of that party, or by use of a product or service 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.



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

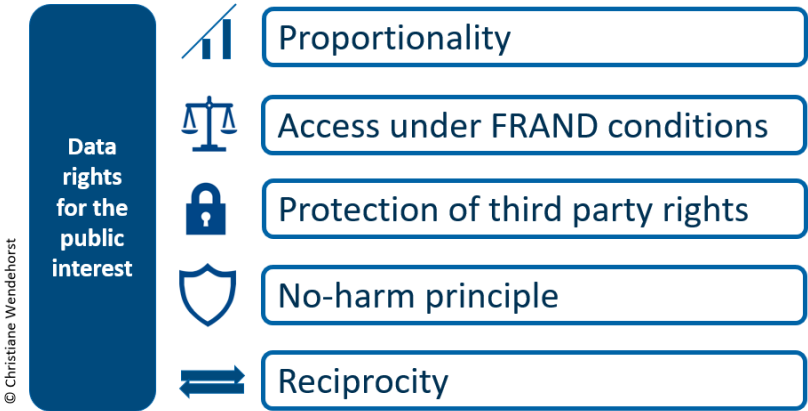
data to desist from particular data uses, are necessary to achieve the desired outcome. According to Principle 21, the fact that the data use is likely to cause significant harm to F is a strong indicator that affording a right to require desistance is justified. However, that alone is normally not sufficient. 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 urging 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 just 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 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 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.

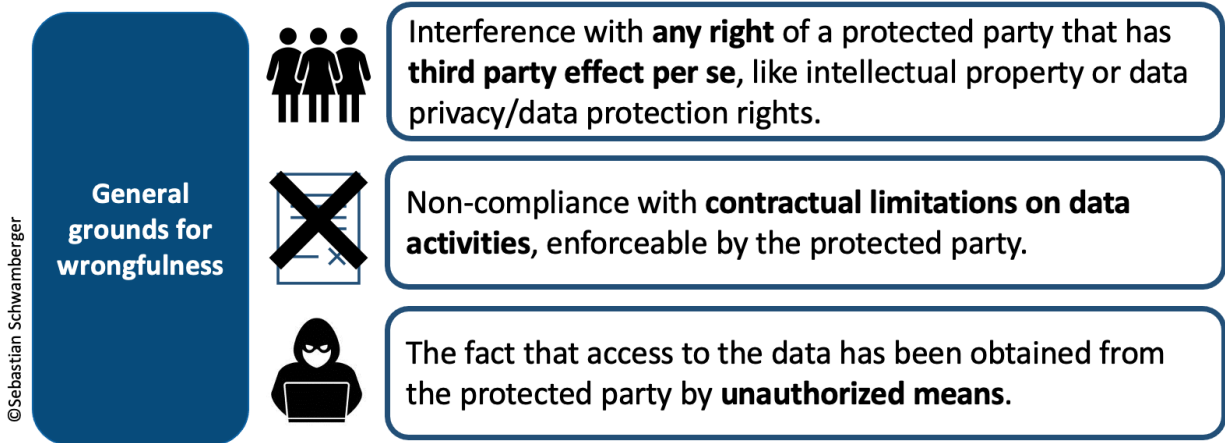
⁹ Recital 40, Regulation (EC) No 1907/2006.

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)

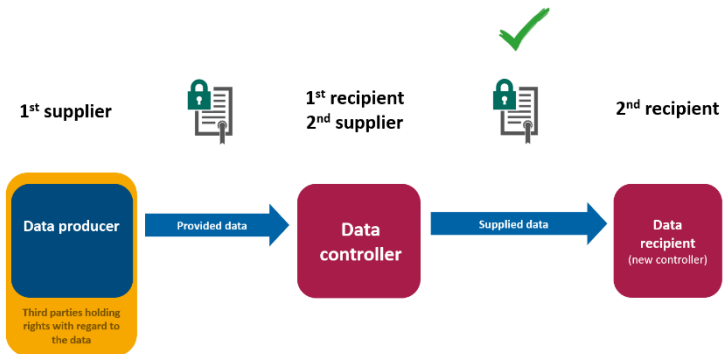
Principle 28 sets out a non-exhaustive list of cases where a data activity is considered to be wrongful:



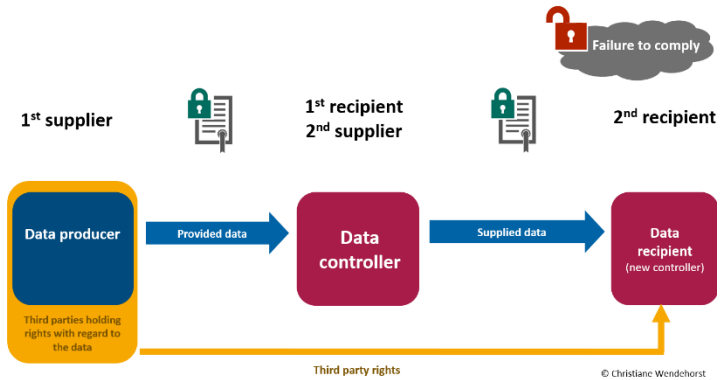
5.2. Effects of Onward Supply on the Protection of Others (Principles 32 – 34)

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 they can prove they have complied with their 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.

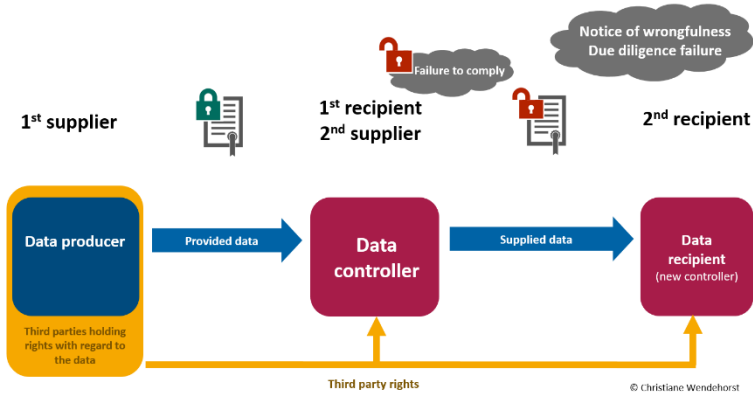


Illustration 4:

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.

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)).

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

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.

Annex: Blackletter of Final Council Draft

As last approved by the ELI Membership on 24 September 2021

Part I: General Provisions

Principle 1: Purpose of these Principles

- (1) The Principles for a Data Economy 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 other 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 the Principles is on records of large quantities of information as an asset, resource or tradeable commodity. The 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 points (a) and (b).
- (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 shall 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 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 assure, as far as is reasonably possible, that the data is permanently inaccessible or otherwise unreadable; and
 - (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’, ‘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’ shall 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) Where these Principles or applicable law would mandate the return or surrender of data by a party (the defendant) to another person (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 the law other than those referred to in paragraph (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 co-exist;
- (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 is to be transmitted electronically to a medium indicated by the recipient, or provided in a way enabling the recipient to port the data to a medium of the recipient's choice, unless either that mode of delivery or the medium indicated is unreasonable in the light of data security concerns in which case the supplier should promptly notify the recipient of those concerns so that the recipient may indicate a substitute mode of delivery or medium.

- (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 which 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 co-operate, 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 which 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 to contracts for the transfer of data, as provided in Principle 5, factors to be taken into account should include, among others:
- (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 where 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 the 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 it 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 the data, 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 access period agreed.
 - (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 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 the data, 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 will 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 which 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

- (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 where, in the 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:**
 - (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.

Principle 11: Contracts for data pooling

- (1) A contract for data pooling is one under which two or more parties (the 'data partners') undertake to share data in a data pool by
- (a) transferring particular data to a medium that is jointly controlled by the data partners or that is controlled by a data trustee or escrowee or other third party acting on behalf of the data partners; or
 - (b) granting each other access to particular data or the possibility to exploit particular data sources, with or without the involvement of a third party.
- (2) This Principle applies, with appropriate adjustments, to the governing principles of any entity created pursuant to a data pooling contract.
- (3) Subject to agreement of the parties and to rules that take priority pursuant to Principle 5, the law should provide that the following terms are included in a contract for data pooling:
- (a) A data partner may utilize data from the data pool, or data derived from such data, only
 - (i) for purposes agreed upon between the data partners in the contract for data pooling;
 - (ii) for purposes which 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 subparagraph (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 the data, unless essentially identical with the original data, 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 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 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 subparagraphs (b) and (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, 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.**

Principle 15: Data marketplace contracts

- (1) A data marketplace contract is a contract between a party seeking to enter into a data transaction (the ‘client’) and a data marketplace provider, under which the data marketplace provider undertakes to enable or facilitate ‘matchmaking’ between the client and other potential parties to data transactions and, in some cases, provide further services facilitating the transaction.**
- (2) Subject to agreement of the parties and to other principles that take priority under Principle 5, the law should provide that the following terms are included in a data marketplace contract:**
 - (a) Insofar as the data marketplace provider undertakes to facilitate or enable a particular step with regard to a transaction, it must provide reasonable support to the client in complying with any legal duties applicable to that step;**
 - (b) The data marketplace provider must refrain from any use for its own purposes of data, received from its client, that is the subject of the anticipated transaction; and**
 - (c) Upon full performance or termination of the contract, the data marketplace provider must erase any data in its control that is the subject of the anticipated transaction and that it has received from its client, and any data derived from such data.**
- (3) In determining which rules and principles to apply by way of analogy, as provided in Principle 5, to data marketplace contracts, consideration should be given in particular to:**
 - (a) whether, and the degree to which, the data marketplace provider gains control of the data concerned; and**
 - (b) whether, and the extent to which, the payment or other performance owed to the data marketplace provider depends on the whether the matchmaking results in a data transaction.**

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 the law other than those referred to in clause (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 who 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 which 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 re-sale 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, where 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 where such development was, in the 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, anonymisation 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 Principles 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; and
 - (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 the public interest, and for similar reasons 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 non-discriminatory 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 Principles 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, inter alia, 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 interfere with 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 over-reaching 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 non-public 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) Where 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 assure that the recipient, and any parties to whom the recipient may supply the data, will comply with those restrictions.
- (2) Where 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 non-waivable by the protected party.

Principle 33: Direct action against downstream recipient

Where an immediate recipient of data had 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 where 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 where (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 where**
 - (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 that 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) Where 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 where 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 non-material non-compliance

- (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 non-compliance 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 has 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 pre-existing 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.**