ELI
EUROPEAN
LAW
INSTITUTE

# Public Consultation on the Data Act

Response of the European Law Institute

ELI

EUROPEAN
LAW
INSTITUTE

Response of the European Law Institute

# Public Consultation on the Data Act

2021

## The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.



European Law Institute Secretariat
Schottenring 16/175
1010 Vienna
Austria
Tel.: + 43 1 4277 22101
Mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

This publication was co-funded by the European Union's Justice Programme. Acknowledgment is also due to the University of Vienna which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011.

Fritz Thyssen Stiftung für Wissenschaftsförderung

Funded by the European Union

universität wien

ISBN: 978-3-9504549-8-7

# Acknowledgements

**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*

**Christiane 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*

# Contents

# 1. Introduction

The Authors are part 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, Tentative Draft No. 2 (which is publicly available[4]), has been approved by the Council and the Membership of the ALI as well as by the Council of the ELI and is currently being submitted for approval to the Membership of the ELI, which has time to cast its vote until 24 September 2021.

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. Especially 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] UNICITRAL 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.

The Authors welcome the opportunity to respond to the public consultation of the European Commission on the Data Act, which aims to establish a legal framework for a fair data economy. The Commission has asked the public on their input on eight measures that are being explored. These are:

I. Business-to-government data sharing for the public interest

II. Business-to-business data sharing

III. Tools for data sharing: smart contracts

IV. Clarifying rights on non-personal Internet-of-Things data stemming from professional use

V. Improving portability for business users of cloud services

VI. Complementing the portability right under Article 20 GDPR

VII. Intellectual Property Rights – Protection of Databases

VIII. Safeguards for non-personal data in international contexts

This response will give an overview on the main Parts and findings of the Principles before elaborating in more detail how they could provide inspiration and guidance in the preparation of the Data Act.

[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://principlesforadataeconomy.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] Jančі 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>.

# 2. The ALI-ELI Principles for a Data Economy

## 2.1. About the Project

### 2.1.1. 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 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 is the reason why 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.

### 2.1.2. 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:

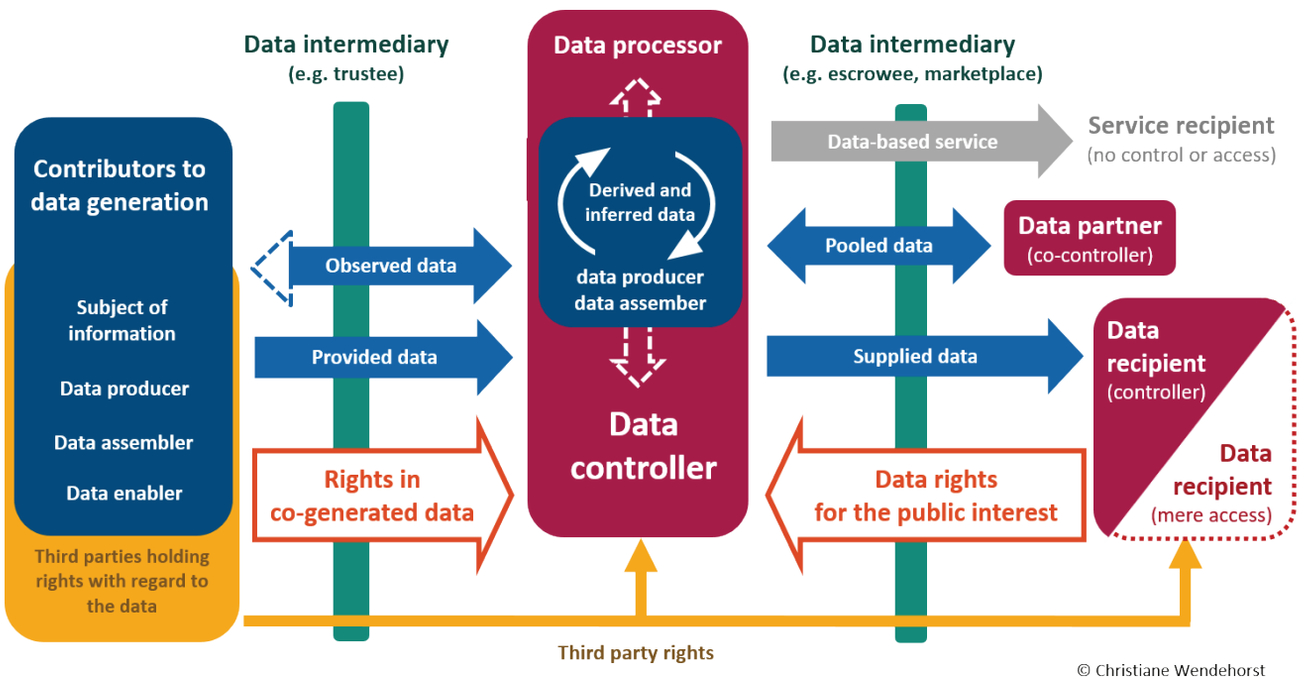



Figure 1: Players in the data ecosystem (simplified)

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.

### 2.1.3. 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) provides default rules for different types of data contracts. 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:

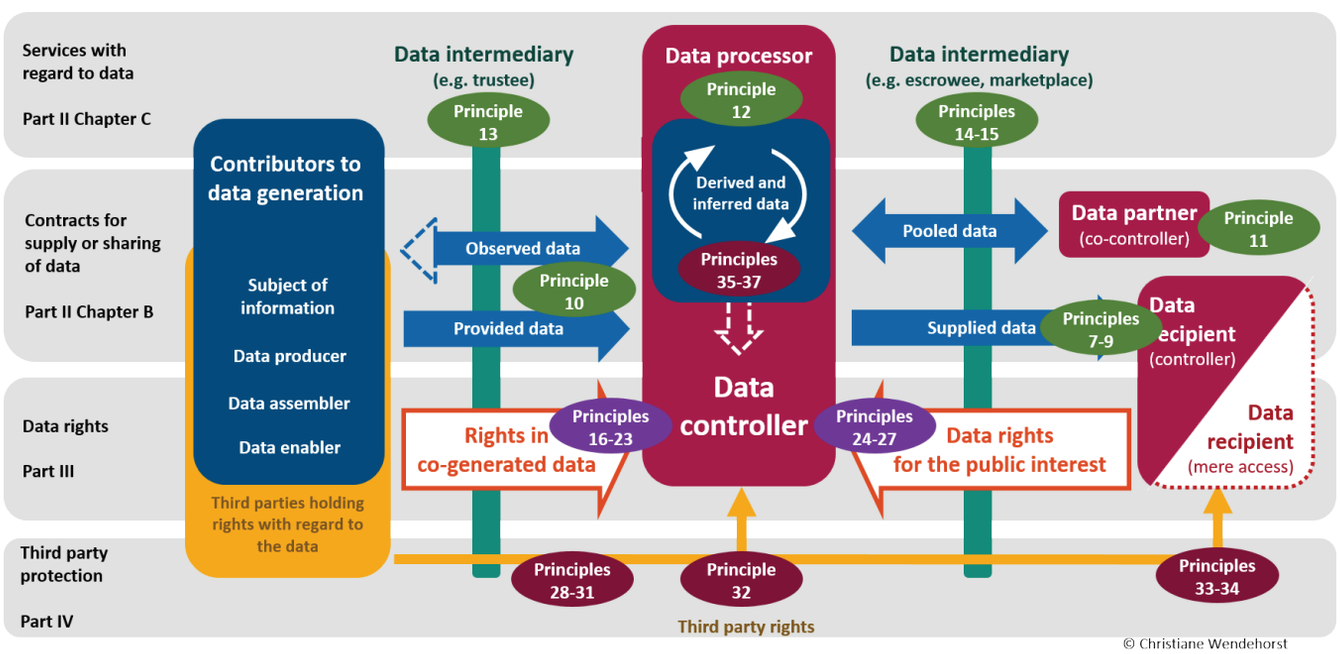



Figure 2: Players in the data ecosystem and how they are addressed by the Principles

## 2.2. 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 core issues that may arise in disputes over data transactions. 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 (sales vs licence approach)? May a party providing services with regard to the data also use the data for their own purposes? The lack of provisions specifically tailored for data transactions is not only bothering parties that want to engage in such transactions, but also 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).

### 2.2.1. 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.

### 2.2.2. 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

With the proposed Data Governance Act[9], the European Commission plans to introduce a legal framework to facilitate the uptake of data intermediation services. 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.

[9] Art 9 ff COM(2020) 767 final.


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


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.

## 2.3. Data Rights (Principles 16 to 27)

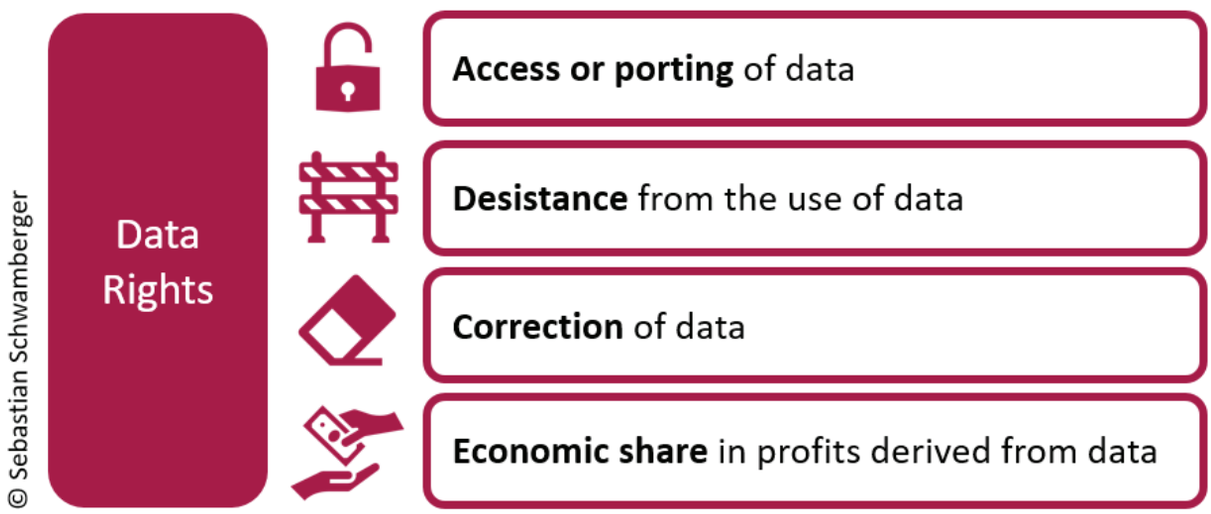
### 2.3.1. Four Data Rights

'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.

### 2.3.2. 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 concrete parties involved, and on a number of factors in the particular situation.

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

#### 2.3.3.1. 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: 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.

© 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.

#### 2.3.3.2. Factors to be considered when granting a data right

The share which a particular party had in the generation

of the data cannot be a sufficient justification for granting a right in the data, such as an access right. Rather, there has to 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.

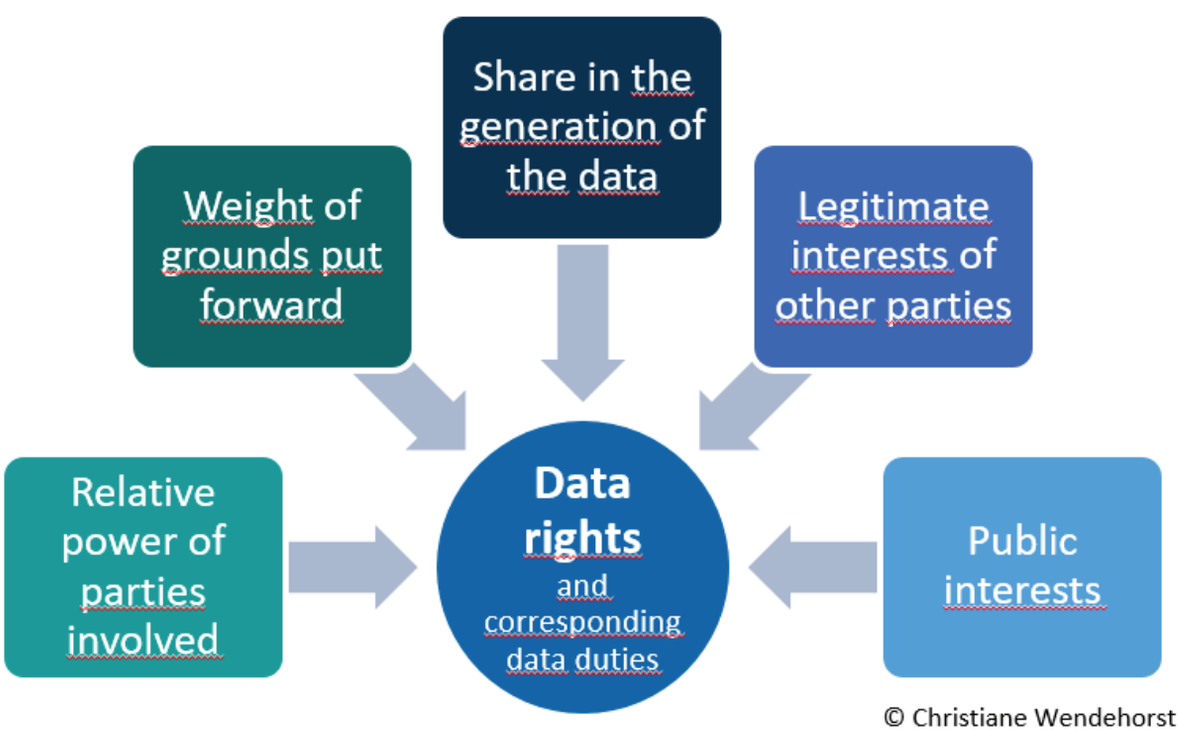
### 2.3.3.3. Legitimate grounds for specific types of data rights

The grounds that can be put forward by the party relying on 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




© Christiane Wendehorst

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 weigh 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 needs 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 a fairer 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.

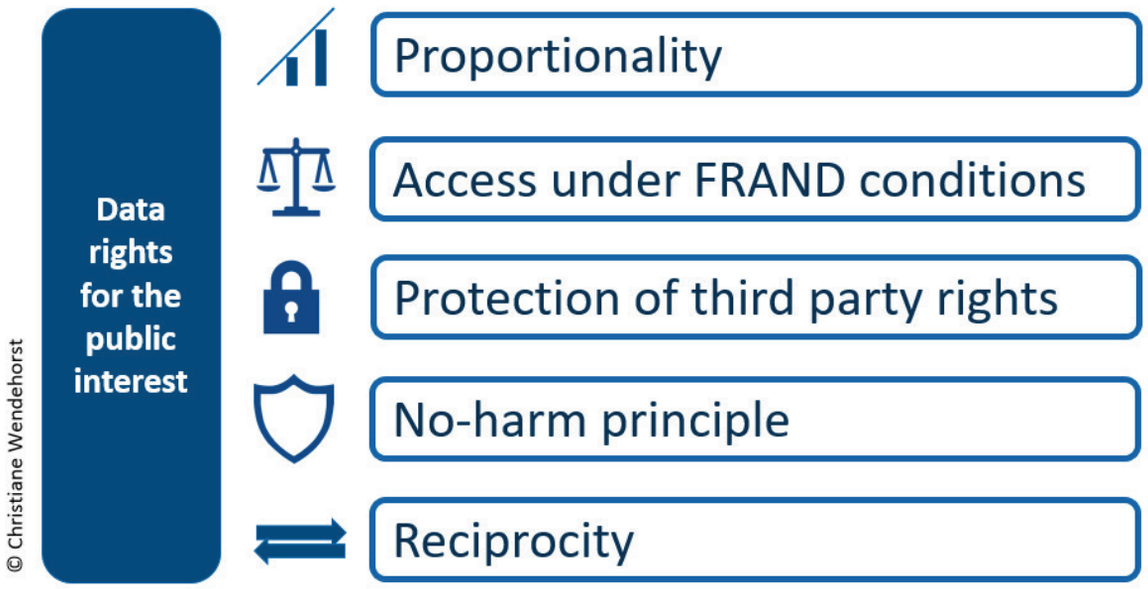
### 2.3.4. Data Rights for the Public Interest and Similar Interests (Principles 24 to 27)

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 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 need to be not only 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 introduction 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 REACH Regulation wants to avoid unnecessary duplication of tests that have a significant impact on our environment and cause unnecessary harm to animals.[10]

Secondly, the law should provide that data rights for

[10] Recital 40, Regulation (EC) No 1907/2006.




the public interests 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, it needs be ensured 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 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 createdfor that purpose.

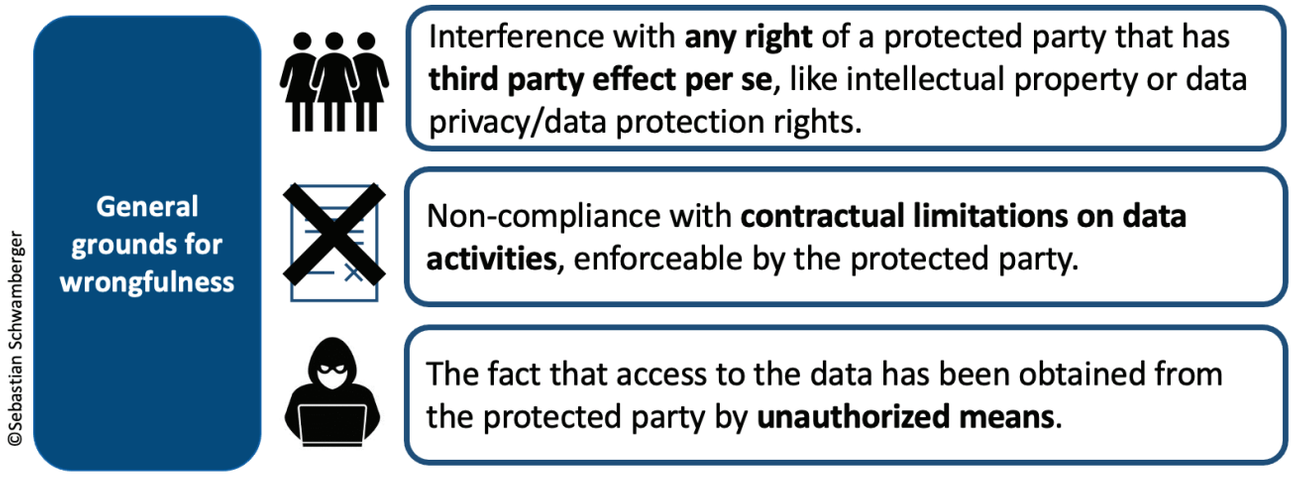
From general considerations of fairness follows that the party receiving data under a data sharing regime for the public interest, should normally be prepared to share similar data under similar conditions with the controller that had originally shared the data (Principle 27). However, whether such a 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.

## 2.4. 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.

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

Inspired by trade secrets protection, Principle 28 sets out a non-exhaustive list of cases where a data activity is considered to be wrongful:




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

The more difficult question of whether and to what extent the wrongfulness of a data activity also affects downstream recipients requires a careful balancing act: 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.

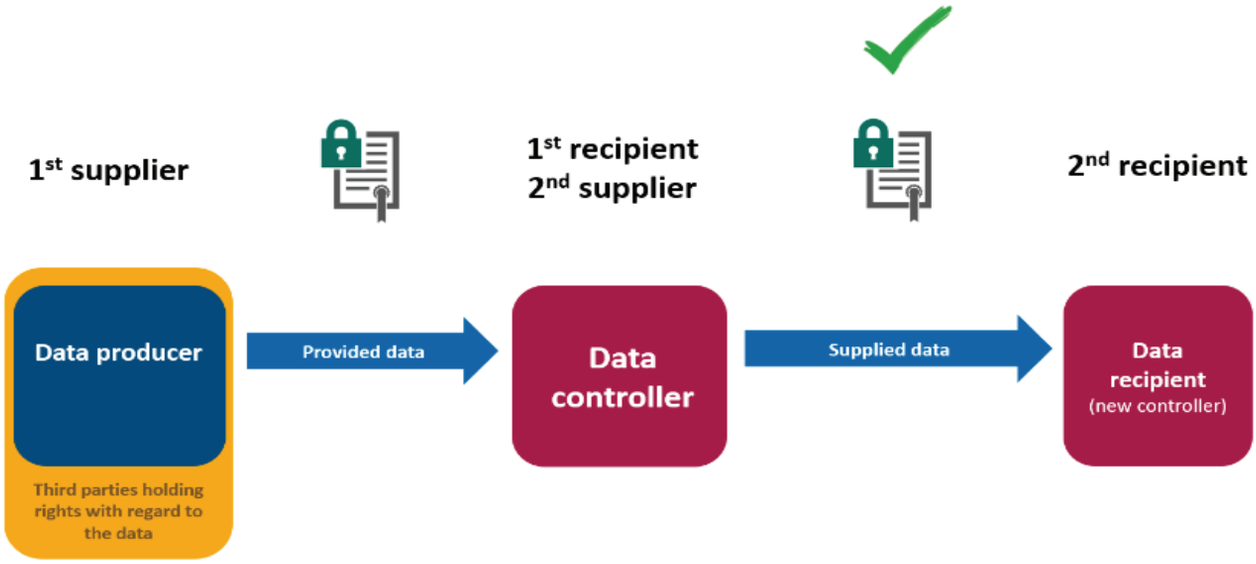
Principle 32 addresses this issue by setting out a duty for any supplier to ensure that recipients will comply with the same duties and restrictions as the supplier. Hence, the supplier, as well as any recipient, who in turn makes data available to further downstream recipients, are obliged to pass on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

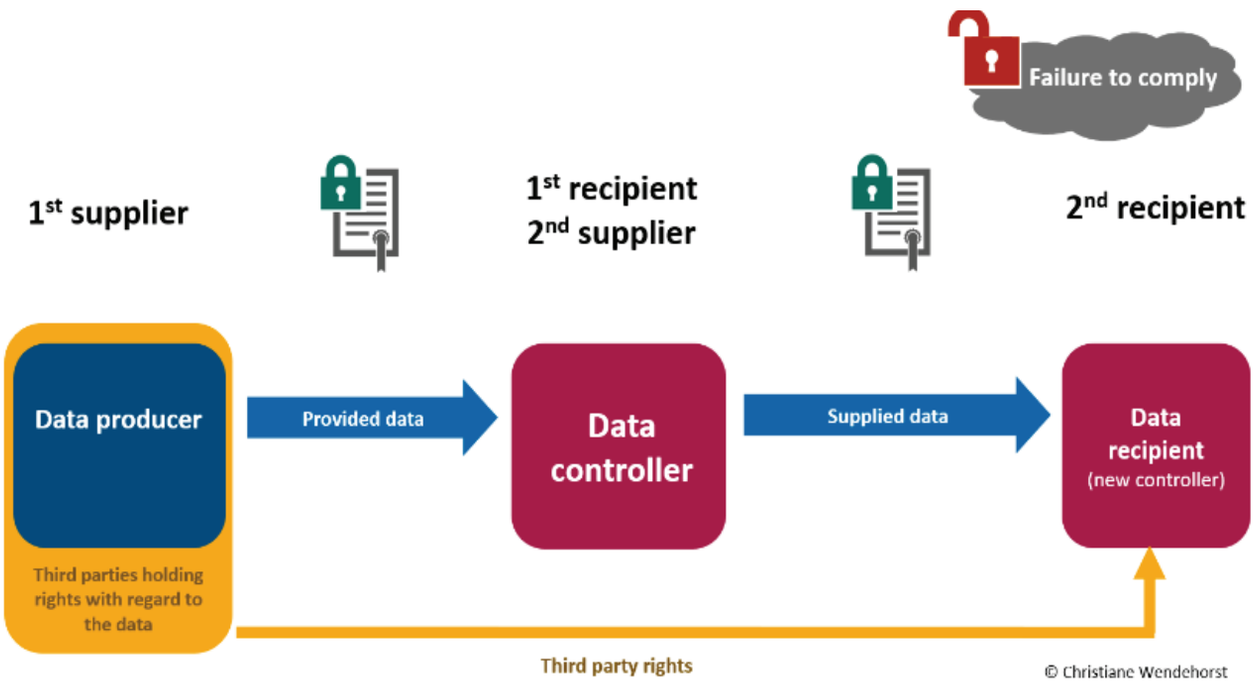
If a downstream recipient infringes protected interests of third parties by engaging in wrongful data activities, the supplier will not be liable vis-à-vis the initial supplier if they can prove they have complied with their duty under Principle 32. However, Principle 33 affords the initial supplier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

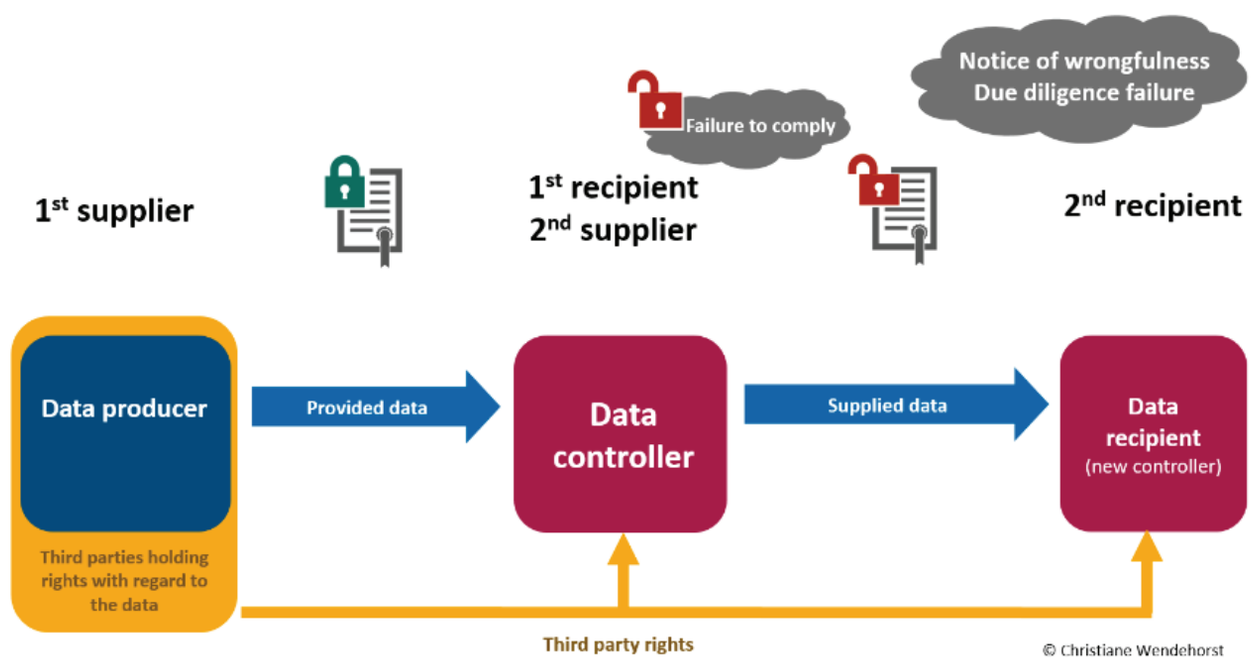
In addition to the grounds of wrongfulness that take direct effect vis-à-vis a downstream recipient (e.g. under applicable data protection law) Principle 34 provides that the data activities of a downstream recipient are wrongful if that recipient had notice or ought to have notice that the supplier 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.


1st supplier
1st recipient
2nd supplier
2nd recipient
Data producer
Provided data
Data controller
Supplied data
Data recipient
(new controller)
Third parties holding rights with regard to the data
© Christiane Wendehorst


Failure to comply
1st supplier
1st recipient
2nd supplier
2nd recipient
Data producer
Provided data
Data controller
Supplied data
Data recipient
(new controller)
Third parties holding rights with regard to the data
Third party rights
© Christiane Wendehorst


Notice of wrongfulness
Due diligence failure
Failure to comply
1st supplier
1st recipient
2nd supplier
2nd recipient
Data producer
Provided data
Data controller
Supplied data
Data recipient
(new controller)
Third parties holding rights with regard to the data
Third party rights
© Christiane Wendehorst

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.

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

Quite regularly, the (downstream) recipient will aggregate the received dataset 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.[11] 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 has to destroy any data or service derived from a wrongful data activity. However, deleting the derived data and stopping the development of the app would lead to the destruction of value that may be unreasonable in light of the circumstances giving rise to wrongfulness. For these cases, Principle 36(2) provides the possibility to keep the data and make an allowance in money instead. The factors that need to be taken into account are (i) whether D had notice of the wrongfulness, (ii) the purpose of the processing, the amount of investment, and (iii) whether the wrongfulness was material and could cause relevant harm to M. Using data to cut emissions is in the public interest and unlikely to harm M's legitimate interests. Hence, D may be afforded the right to make an allowance in money instead of erasing the wrongfully derived data. The same holds true for the app that is being developed with the help of the derived data (Principle 36(3)).

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

[11] See Article 4(1), Recital 26 GDPR (Regulation (EU) 2016/679)

# 3. Guidance to be Derived from the Principles for the Data Act

While the ALI-ELI Principles for a Data Economy have not been drafted with the specific questions posed in the public consultation on the Data Act in mind, and while they follow a different structure and terminology, the Authors believe that the Principles can provide a certain degree of guidance on several of the questions raised.

## 3.1. Business-to-government (B2G) data sharing for the public interest

At the turn of the century, the public sector was the biggest single data holder[12] – today, the largest datasets are held by private actors. The European Commission's plan to enhance data sharing between private businesses and the public sector in order to utilise the untapped potential of privately held data in a way that benefits society as a whole is much supported by the Authors. While the Principles do not specifically address B2G data sharing, Part III Chapter C on data rights for the public interest can also be used as guidance for horizontal B2G data sharing requirements. The considerations in Chapter C overlap to a great extent with the key principles already identified by the Commission in its Communication 'Towards a Common European Data Space'.[13] Given the variety of public interests potentially at stake, the Data Act, as a horizontally conceived piece of legislation, will not be able to provide specific guidance as to the circumstances under which such data sharing obligations may be imposed. However, the Data Act can very well define and harmonise the core aspects that need to be considered when deciding whether to impose B2G data sharing obligations.

To ensure that the interests of data holders are duly taken into account, the Data Act will need to set out a proportionality test for B2G data sharing obligations. Only where a public body can clearly demonstrate that the request for data access under Data Act pursues a legitimate public interest and is necessary and proportionate, an encroachment of the data holder's interests is justified. When determining the weight of the public interest, factors identified by the Commission's High Level Expert Group on B2G Data Sharing should be taken into account: (i) likelihood of the benefits, (ii) intensity of the likely benefits, (iii) immediacy/urgency of the situation, (iv) potential harm of the non-use of data, and (v) whether other possibility to have access to the data exist.[14] The public interest needs to be balanced not only against the interests of the controller but also against that of protected third parties that may be affected by the sharing obligation, such as data subjects or holders of IP rights. In particular, the likelihood and intensity (number of people affected, sensitivity of the data) of harms for protected third parties need to be considered.[15] Furthermore, costs and effort required

[12] COM(1998) 585 final..
[13] COM(2018) 232 final.
[14] Expert Group B2G Data Sharing, 44.
[15] ibid.

for the supply and re-use of private sector data should be reasonable compared with the expected public benefits.[16]

The considerations of the proportionality test should not only be decisive for whether access is granted or not, but also for how the access is granted. This includes important modalities, such as limitations on how and for how long the data may be used, restrictions for the protection of third parties, support by the business required to share the data, or remuneration to be paid. The Data Act should ensure that costs arising from the data sharing obligation are normally borne by the public body, subject to narrowly-defined exceptions (e.g. a gatekeeper platform is under a duty to share data with researchers), and that any financial losses incurred by the business sharing the data are compensated. Remuneration beyond compensation of costs, however, is only justified if the data was generated with significant efforts by the data holder. Hence, granting none or only limited remuneration to a company that is under a B2G sharing obligation can be justified if no significant investments were made and the data sharing obligation is not likely to cause any financial losses.

The framework for data sharing in B2G should include a strict rule on purpose limitation. Other than beneficiaries of B2B data access rights in the public interest (see 3.3), public actors should be allowed to use the data exclusively for the purposes for which the right had been afforded. In addition, any use of the data in a way that may harm the legitimate interests of the original controller more than is inherent in the purpose for which the access right was afforded should be explicitly prohibited.[17] Such provisions would minimise not only the encroachment of the data holder's legitimate interests but also ensure trust in the data activities carried out by public bodies. For example, financial data of private actors that is accessed by a public authority in order to identify and analyse gender pay gaps may not be shared with tax authorities.

As proposed by the Expert Group on B2G data sharing, the Data Act should also provide for transparency obligations on both the supply side (those that have the data) and the demand side (those that need the data). Transparency obligations for companies could help the public sector identifying data that can benefit society at large. Without insights into quality, type, size, and other characteristics of privately held datasets, much of the potential this data holds may be left untapped. It goes without saying, however, that such transparency obligations need to ensure that data holders' legitimate interests are duly protected. On the demand side, it has already been pointed out that the legitimate interest, as well as necessity and proportionality, must be clearly demonstrated. In addition, public bodies should disclose the data activities performed on the data and the derived results, unless such disclosure would be contrary to the public interest. This would not only ensure the accountability of the public body but also increase trust.[18]

## 3.2. Business-to-business (B2B) data sharing

### 3.2.1. Three different challenges and scenarios

The European Data Strategy (COM(2020) 66) intends to promote B2B data sharing, which will benefit in particular start-ups and SMEs, putting emphasis on facilitating the voluntary sharing of data on the basis of contractual arrangements. The Proposal for a Data Governance Act (COM(2020) 767) seeks to establish a framework for data intermediation services that may support businesses in sharing their data with others. However, what is so far missing is standards that ensure conditions of data sharing between a holder of data and a (potential) recipient of data are fair.

It is important to stress that the need to ensure fairness in the relationship between holders and recipients, or between holders and potential recipients, arises mainly in three different scenarios, and that there are thus mainly three different challenges to address:

i) A holder of data is considering to share data with others but is discouraged by legal uncertainty or by lack of protection against particular risks (the "discouragement by risks and uncertainty" scenario);

ii) Parties are in a contractual relationship with each other, or belong at least to the same economic ecosystem (such as by being links in a value chain), but data access and use occur under conditions that are unfair vis-à-vis weaker parties (the "unequal bargaining power" scenario);

[16] COM(2018) 232 final.
[17] Principle 25(2).
[18] Expert Group B2G Data Sharing, 46.

iii) The law mandates a data sharing obligation, or the parties agree in principle on data access, but everyone feels uneasy about it because there is a lack of clear guidance with regard to access modalities (the "guidance on horizontal access modalities" scenario).

The appropriate responses to the three different scenarios or challenges overlap to some extent, but they are not necessarily identical.

### 3.2.1. The "discouragement by risks and uncertainty" scenario

Where a holder of data is, in principle, considering to share data with others but is discouraged by legal uncertainty or by lack of protection against particular risks, appropriate responses may be the provision of optional model contract terms and other support measures for parties in the data economy, default terms for data transactions, and/or (mandatory) legal rules creating certainty about third-party aspects of data activities.

#### 3.2.1.1. Option 1: Optional model contract terms and other support

The first and least invasive option to incentivise fair B2B data sharing would be to provide sets of purely optional model contract terms and other practical support (such as legal and technical information and advice or the provision of data sharing infrastructures) for parties in the data economy. The model contract terms would function as templates that actors in the data economy could use when entering into data transactions. Since the model terms would be mere recommendations and not binding law, they would not cause any disruptive effects for national and EU private law.

It is in order to provide this kind of support that the European Commission initiated and funded the establishment of a "Support Centre for Data Sharing" (SCDS).[19] So the question arises whether the European Commission should continue relying on the SCDS. It could also go much further and publish, by way of Commission Decisions, standard contractual clauses similar to those published for personal data transfers to recipients outside the territorial scope of the GDPR (SCC),[20] or take any other action in between these two ends of the spectrum.

The Authors believe that the provision of model contract terms beyond what has so far been provided by the SCDS could greatly assist smaller players in the data economy in sharing data where they can themselves choose the terms, and in assessing the fairness of terms presented to them by other players. They are, however, not sure whether SCC published in the Official Journal are the right format. The situation with B2B data sharing in general is different from the situation with personal data transfers outside the territorial scope of the GDPR in various respects: The SCC are designed to serve data protection as their only goal, they address a standard situation defined by a clear legislative setting in the GDPR, and a situation where the need to ensure compliance with the GDPR is in itself a sufficient incentive for parties to use the SCC. By way of contrast, the range of possible constellations where B2B data sharing may be desirable is close to infinite, legal and economic requirements differ from case to case, and parties (and their lawyers) may prefer bespoke agreements in any case.

This is why the Authors believe that more flexible solutions, such as "Guidelines for B2B Data Sharing" produced by or on behalf of the European Commission, are preferable. If the Commission were to choose this policy option, the default rules in Part II of the Principles (plus Principle 32 for third party protection) could be used as a source of inspiration, alongside other materials, including the Guidelines issued by the Japanese Ministry for Economy, Trade and Industry (METI).[21] The default rules in Part II could inform the drafting of Guidelines both in terms of the standard types of transactions to be addressed and in terms of the model contractual clauses recommended for each type of agreement.

By way of example, this could be introduced in the future Data Act in conjunction with a general transparency rule for standard terms and conditions, which is inspired by Part II of the Principles:

[19] https://eudatasharing.eu/. The SCDS is run for the European Commission by a consortium of three companies: Capgemini Invent, Fraunhofer Fokus and Timelex.

[20] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council OJ L 2021/199, 31.

[21] METI, Contract Guidelines for Utilization of Data and AI, https://www.meti.go.jp/english/press/2019/0404_001.html.

**CHAPTER II: Business-to-Business Data Sharing**

**Article 4[1]: Voluntary data sharing among businesses**

(1) Businesses sharing data with other businesses, requesting the sharing of data from other businesses, or acting as data intermediaries between suppliers and recipients within the meaning of Article 9 of the Data Governance Act, on the basis of standard terms and conditions shall set out in their terms and conditions, in a clear and transparent manner, at least

a) the way in which the recipient will be granted access to the data;

a) any warranties or their absence with regard to data quantity or quality;

b) any warranties or their absence with regard to the legal position the recipient will have in respect of the data, including in respect of intellectual property rights;

c) the ways in which the recipient will be allowed to utilize the data or, if the ways cannot be described in advance, whether contractual limitations apply;

d) the distribution of responsibilities, as between the parties, for compliance with legal requirements and any steps that may be required for the protection of third parties.

(2) To facilitate the compliance of businesses with the requirements of this Article, the Commission shall accompany the transparency requirements set out in this Article with guidelines.

[1] Numbers of Chapters and Articles are purely fictional. The Authors have chosen to begin with Article 4 as the first Articles of a legal instrument are normally devoted to issues such as purpose, scope, and definitions. The Authors wish to stress that no pre-drafts of whatever kind have been disclosed to them, and that they have not prepared any full draft.

The Authors recommend that the Guidelines address, at least, the following five types of data transactions separately:

- Contracts for the transfer of data (Principle 7)
- Contracts for mere access to data (Principle 8)
- Contracts for authorisation to access (Principle 10)
- Contracts for data pooling (Principle 11)
- Data trust contracts/Contracts for data intermediation services (Principles 13/15)

It is to be borne in mind, however, that the default rules in Part II were never designed to completely replace contractual agreements, i.e. model contractual terms and any Guidance on drafting data contracts would possibly have to address a range of additional issues.

#### 3.2.1.2. Option 2: Default rules for data contracts

Introducing default rules (implied terms, default terms)[22] for data contracts would go one step further than Option 1. Unlike model terms, default rules would 'automatically' be included in a contract unless derogated from by agreement of the parties. Hence, they could help solve disputes with regard to the rights and obligations of parties that arise over issues accidentally or intentionally omitted by the agreement of the parties. While model terms and default rules both save transaction costs, default rules, due to their 'automatic' gap filling function, would have more practical relevance than model terms.

Default rules with regard to B2B data sharing could be greatly inspired by the default terms proposed by Part II of the Principles.

However, given the absence of default rules at European level for the vast majority of other transactions, and the fact that such default rules would therefore be an alien element in the acquis that might cause disruption with national contract laws, the Authors generally recommend guidelines (Option 1) instead of default rules (Option 2).

#### 3.2.1.3. Option 3: Legal protection and certainty in data value chains (in addition to Option 1 or 2)

Neither model contract terms nor default rules can protect the contracting parties from legal risks originating from outside their contractual relationship. The Authors therefore believe that the issue of discouragement by risks and uncertainty cannot be addressed on the contractual level alone. A number of concerns that discourage parties from engaging in B2B data sharing, including

- the concern of the data holder that the recipient will pass the data on to third parties, or that third parties may get unauthorised access to the data, and that there is, in the absence of IP protection for most data, no protection against data activities by those third parties; and
- the concern of the data recipient that there are issues with the data and that those issues may ultimately mean that value the recipient has created with the data will be destroyed and investment be frustrated,

cannot be addressed by ensuring fairness in the agreement between data supplier and data recipient, as legitimate interests of third parties come into the equation. This can only be addressed by way of mandatory rules addressing the type of issues dealt with by Part IV of the Principles that aim at creating legal certainty about third party aspects of data activities, including with regard to rights an upstream supplier or another third party can have against downstream recipients, and with regard to the effects of data processing activities on third party rights.

There are many different ways in which such rules could be drafted, and they would not have to be part of the Data Act, but could equally be included in a separate Chapter of the Trade Secrets Directive. Just by way of illustration, this is what a "translation" of Part IV of the Principles into rules could look like:

[22] Austrian and German: dispositive Rechtsvorschriften, Dutch: aanvullende rechtsregels or regelend recht, French: régles de droit supplétives, Italian: norme dispositive, Spanish: normas dispositivas.

**CHAPTER III: Protection of Third Parties**

**Article 8: Protection of third parties in the sharing of data**

(1) Where a holder of data is subject to any duties or restrictions with regard to the data, including duties and restrictions following from

a) data protection law;

a) intellectual property or trade secrets law;

b) contractual arrangements with third parties; or

c) the fact that data has been obtained by unauthorized means, in particular by a criminal act under the Budapest Convention

that holder must make sure any sharing of data with other parties is consistent with those duties or restrictions.

(2) Unless provided otherwise by the relevant legal regime, the holder of data must

a) impose the same duties and restrictions on the recipient as the holder is subject to (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

d) 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.

(3) Where the initial holder of data later obtains knowledge of facts that indicate wrongful data activities 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.

(4) The duties under this Article are without prejudice to any strict vicarious liability for data activities by a recipient under the applicable law.

**Article 9: Direct action against downstream recipient**

Where an immediate recipient of data had a duty under Article 8 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.

**Article 10: Wrongfulness taking effect vis-à-vis downstream recipient**

(1) 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 Article 8 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

e) 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 protected party;

f) 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 protected party; or

g) 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.

**Article 11: Protection of third parties in the processing of data**

(1) If a controller may process data but is obligated to comply with duties and restrictions of the kind addressed in Article 8(1), 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

h) 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) 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.

(3) To the extent that undoing the processing in cases covered by paragraph (2) 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 protected party, 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;

i) the purposes of processing;

j) whether wrongfulness was material in the circumstances or could be expected to cause relevant material harm to a party protected under Chapter A; and

k) the amount of investment made in processing, and the relative contribution of the original data to the derived data.

(4) Paragraphs (2) and (3) apply with appropriate adjustments to products or services developed with the help of the original data.

**Article 12: 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 for the protection of third parties 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;

l) the controller has made the efforts that could reasonably be expected in the circumstances to comply with the duties and restrictions; and

m) the data activities are not related to the purpose for which duties or restrictions 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.

### 3.2.2. The "unequal bargaining power" scenario

#### 3.2.2.1. Option 1: General unfairness test for data access and use

Where the issue preventing B2B data sharing is not so much that of discouragement, but the fact that a party with dominant bargaining power refuses data access to a weaker party (or takes access to data held by that weaker party and uses that data) in a manner that is unfair, additional measures need to be taken. These measures must include an unfairness test.

One option would be to introduce, in the Data Act, just a general unfairness test for data access and use. It is to be stressed that such an unfairness test could not restrict itself to unfair contractual clauses but would have to be extended to unfair practices in commercial dealings as the problem is often not so much the existence of a contract term, but rather its absence. Also, declaring a contract term invalid does not automatically fill the emerging gap, in particular not in the absence of default rules on data access and use. This is why the Authors recommend introducing a fairness test for both contractual terms and practices.[23] They do not recommend that such a fairness test be limited to the IoT sector, but rather that it be adopted on a horizontal basis, even though the IoT sector will be the most important context in which issues arise.

The general factors to determine co-generation of data and factors to be taken into account for determining data rights set out by Principles 18 – 19 can provide guidance in that regard. By way of illustration, the concepts and ideas reflected in those Principles could be implemented as follows:

[23] See also the approach taken in the Late Payments Directive and the Unfair Trading Practices in the Food Supply Chain Directive.

**Article 2: Definitions**

For the purpose of this Regulation, the following definitions apply:

….'co-generated data' means data to the generation of which two or more parties have contributed as set out in more detail in Article 5;

…

**CHAPTER II: Business-to-Business Data Sharing**

**…**

**Article 6: 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 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;

a) 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;

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

c) 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.

**Article 7: Unfair contractual terms and commercial practices with regard to co-generated data**

(1) A contractual term or a commercial practice relating to the granting or denial of access to co-generated data, or to the use of co-generated data, is either unenforceable or gives rise to a claim for damages if it is grossly unfair to a party that has a share in the generation of the data, contrary to good faith and fair dealing. This includes contractual terms or practices with regard to specifications or restrictions of data access or use, including concerning modalities of access and types of permissible use, data formats, timing, data security, further support required for effective access or use, and remuneration to be paid.

(2) In determining whether a contractual term or a commercial practice is grossly unfair to a party that has a share in the generation of the data, within the meaning of the first subparagraph, all circumstances of the case shall be considered, including:

a) the share which that party had in the generation of the relevant data, considering the factors listed in Article 6;

d) the weight of grounds such as those listed in Annex IB which that party can put forward for being afforded the data right;

e) the weight of any legitimate interests the controller or a third party may have in denying the data

right;

f) imbalance of bargaining power between the parties; and

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

(3) – (4) …

(5) A claim for damages under paragraph (1) primarily includes a right to be afforded access to the relevant data, or to require desistance from the relevant data use, unless this is impossible or clearly inappropriate in the circumstances, in which case damages will be due in money.

As far as there is a right to be afforded access to data under subparagraph 1 such right 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. In any case, the party affording access to data must comply with the duties under Article 8 for the protection of third parties.

#### 3.2.2.2. Option 2: General unfairness test combined with a grey and/or black list

In addition to a general unfairness test, the Commission may also wish to consider a grey and/or black list with terms or practices that are presumed to be unfair (grey list) or that are always considered to be unfair (black list). A grey list does not amount to an outright ban, as it can still be argued that the use of grey listed practices or terms is justified in the concrete circumstances. The list should not be limited to contractual terms but also include commercial practices. As the grey list needs to apply to situations across various sectors, the terms and practices included in the list should be held general rather than overly specific.

The legitimate grounds for exercising data rights set out by Principles 20 – 23 can provide guidance in that regard, but the exact division between terms and practices to be greylisted and terms and practices to be blacklisted would require further debate. Just by way of illustration, this is how the Principles could be implemented:

**Article 7 : Unfair contractual terms and commercial practices with regard to co-generated data**

…

(3) The contractual terms or commercial practices listed in Annex IA shall be considered unfair under all circumstances.

(4) The contractual terms or commercial practices listed in Annex IB shall be presumed to be unfair unless it can be demonstrated that a term is not unfair in the circumstances.

**…**

**Annex IA:**

A contractual term or commercial practice shall be considered unfair under all circumstances within the meaning of Article 7(3) if its aim or effect is to

a) deprive the end user of a product or service of access to co-generated data that would be necessary for normal use, maintenance or re-sale by the user of a product or service consistent with its purpose;

b) deprive the end user of a product or services of the data necessary for switching suppliers of products or services;

c) …

**Annex IB:**

A contractual term or commercial practice shall be presumed to be unfair within the meaning of Article 7(4), if it is not already considered unfair in all circumstances under Article 7(3) and Annex IA, and if its aim or effect is to

a) cause, or be likely to cause, significant harm, including non-economic harm, to the other party and the term or practice is inconsistent with the way that party contributed to the generation of the data; this includes cases where that party was induced to contribute for an entirely different purpose and could not reasonably have been expected to contribute if it had known or foreseen the term or practice, and cases where that party's contribution was obtained by deceit, duress or undue influence;

b) deprive a party of the data necessary for switching suppliers of products or services or attracting further customers;

c) deprive the supplier of a product or service with access to data that would be necessary for quality monitoring or improvement of that product or service consistent with duties of that supplier;

d) deprive a contracting party from access to data that is 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 cannot reasonably be expected to harm the controller's interests;

e) deprive a party of the data necessary for the development of a new product or service where such development was, in the light of the parties' respective 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;

f) …

#### 3.2.2.3. Option 3: Combination of Option 1 or 2 with default rules on data rights

In combination with Option 1 (general unfairness test only) or Option 2 (general unfairness test plus grey and/or black lists of terms and practices), the Commission may also choose to put forward default rules that would both fill gaps in incomplete agreements and function as a benchmark and point of orientation for unfairness control by the courts. Parties to a contract would be able to deviate from the default rules whenever it is in their best interest to do so. However, deviations from or exclusions of the default rules would be limited to the extent that they must not lead to unfair results. The factors that should be taken into account to determine whether a deviation from a default term is unfair should be the same as under Options 1 and 2.

One of the main differences of Option 3 as compared with Options 1 and 2 is that, under Option 3, the parties would not have to invest in the drafting of contractual clauses if they find that the statutory default regime serves their interests and needs. Conversely, they have to invest in the drafting of contractual clauses that deviate from the statutory default regime if they find that the statutory default regime is not (fully) appropriate to meet their needs. Another difference of Option 3 as compared with Options 1 and 2 is that one would not need a 'detour' via a claim for damages in order to achieve the desired result of affording a party access or achieving desistance from particular data activities. Rather, the data right as such would already follow from the default rules as a baseline regime. This could, by way of illustration, be phrased as follows:

**Article 7*: Rights in co-generated data**

(1) In the case of co-generated data, a party who had a role in the generation of the data has a right to access the data, or to require that the holder of the data desist from a particular data use, when it is fair and 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 Article 6;

a) the weight of grounds such as those listed in Annex IA* and Annex IB* which that party can put forward for being afforded the data right;

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

c) imbalance of bargaining power between the parties; and

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

(2) The factors listed in paragraph (1) 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.

(3) As far as there is a right to be afforded access to data such right 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. In any case, the party affording access to data must comply with the duties under Article 8 for the protection of third parties.

**Article 7*bis** : Unfair contractual terms and practices with regard to co-generated data***

(1) A contractual term or a practice relating to the granting or denial of access to co-generated data, or to the use of co-generated data, is either unenforceable or gives rise to a claim for damages if it is grossly unfair to a party that has a share in the generation of the data, contrary to good faith and fair dealing.

(2) In determining whether a term or practice is grossly unfair the factors in Article 6 with Annexes IA and IB should be taken into account.

**Annex IA*:**

Grounds to be put forward by a party for being afforded a right to access co-generated data within the meaning of Article 7*(1)(b) include, but are not limited to, the data being necessary for

a) switching suppliers of products or services or attracting further customers;

e) for normal use, maintenance or re-sale by the end user of a product or service consistent with its purpose;

f) quality monitoring or improvement of a product or service by the supplier of that product or service, consistent with duties of that supplier;

g) establishing facts, such as better understanding of a 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 cannot reasonably be expected to harm the controller's interests;

h) the development of a new product or service where such development was, in the light of the parties' respective 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;

i) …

**Annex IB*:**

Grounds to be put forward by a party for being afforded a right to require desistance from a particular data use within the meaning of Article 7*(1)(b) include, but are not limited to, that data use

a) causing, or being likely to cause, significant harm, including non-economic harm, to the other party and the term or practice is inconsistent with the way that party contributed to the generation of the data; this includes cases where that party was induced to contribute for an entirely different purpose and could not reasonably have been expected to contribute if it had known or foreseen the term or practice, and cases where that party's contribution was obtained by deceit, duress or undue influence;

…

The Authors want to stress that, even though Option 3 is even closer to the original wording of the Principles, they tend to favour Option 2., as they believe the very flexible factors that are to be taken into account when deciding about data access or use are better suited for an unfairness test than for a statutory right. There may be good arguments for introducing hard and fast data access rights, for the time being, only in sectoral legislation.

## 3.3. The "guidance on horizontal access modalities" scenario

The Commission is considering introducing horizontal access modalities that would regulate in a harmonized way how data access rights should be exercised while the possible creation of sectoral data access rights would be left to future sectoral legislation, where justified. The Authors very much welcome this approach, as, while they agree data access rights should largely be implemented in sectoral legislation, this could easily lead to inconsistent results and to more incoherence in areas that are already subject to various overlapping pieces of legislation. Establishment of horizontal access modalities is particularly important where data access rights are not justified by the share the party seeking access had in the generation of the data (because modalities would then be determined by the same factors as the data right itself, see above at 3.2.2) but in the public interest. However, given that the dividing line between both types of data access rights is often blurred, horizontal access modalities could be helpful also for access to co-generated data.

Generally speaking, statutory data access rights, in particular where not based on the notion of co-generation but on the public interest, must be consistent with the proportionality principle. This proportionality test applies not only to whether or not a right should be afforded and/or an obligation imposed, but also to any specifications or restrictions, such as concerning data formats, mode of access, timing, data security, further support required for exercise of the right to be fully effective, and remuneration to be paid.

An important factor to be duly taken into account when considering modalities is whether the data right for the public interest encroaches not only the rights of the controller but also affects the protected interests of other parties, such as data subjects (in the case of personal data) or the holders of IP rights (where the data is IP protected). The different modalities that are necessary if personal data is involved can be illustrated by comparing the access rights of the Type Approval Regulation[24] and the Payment Services Directive II.[25] Article 61 Type Approval Regulation gives independent maintenance and repair service providers a right vis-à-vis car manufactures to access the technical information necessary to perform their services. The provision is justified by the public interest of preventing a market failure on the aftermarket, which would lead to higher prices,

[24] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers and, and of systems, components and separate technical units intended for such vehicles, OJ L 2018/151, p. 1.

[25] Directive (EU) 2015/2366 on payment services in the internal market, OJ L 2015/337, p. 35.

lower quality of services, less innovation, and less choice for consumers. The PSD II's so-called 'access to account' rule allows third-party providers to access the account information of customers in order to provide payment initiation or account information services if the customers have given their explicit consent. Since the account data, other than technical data under the Type Approval Regulation, is personal data, the access right not only affects the interests of the bank but also those of the customers. The interest of the general public in more innovative payment services may not simply overrule the interest of individual payers, who might prefer the protection of their privacy over new ways of transferring their money. By subjecting the data access of payment service providers to the consent of the payers, their interests are sufficiently protected. Examples of other restrictions that could be introduced to protect the interests of others when affording a data right are disclosing data only to a trusted third party as well as the disaggregation, anonymization or blurring of data (Principles 25(2)).

Where data access rights for the public interest are afforded, 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 (Principle 25(1)). Where sector-specific access rights are afforded, the law could provide either that the data may be used exclusively for the purposes for which the right had originally been afforded or can be more open with regard to data use. The Data Act should, as a ground rule, follow the latter approach and allow the use of the data in any lawful way and for any lawful purpose as long as this is consistent with the public interest for which the right was afforded, restrictions for the protection of others and any agreement between the parties (Principle 26 (1)). This approach would allow to better help foster innovation and growth in the data economy. The general freedom of use should, however, be limited by a no-harm rule, which restricts utilisation of the 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. An example for harm that is inherent in the purpose is the original controller's competitive losses if an access right is introduced to counter competitive distortions (Principle 26(2)).

By way of illustration, this is how such general access modalities could be phrased, drawing inspiration from Part III, Chapter C of the Principles:

**CHAPTER II: Business-to-Business Data Sharing**

....

**Article 5: Data sharing among businesses on the basis of statutory data sharing obligations**

(1) Where a business shares data with another business on the basis of a statutory sharing obligation, the modalities of data access by the recipient must be necessary, suitable and proportionate to the public interest pursued, taking into account the legitimate interests of the data holder and third parties. This includes, inter alia, data formats, timing, data security, further support required for exercise of the right to be fully effective, and remuneration to be paid.

(2) Data access must 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. In any case, the party sharing the data must comply with duties under Article 8, and no data sharing obligation may be imposed that would prevent that party from complying with those duties.

(3) If the law imposes a data sharing obligation the holder must provide access under conditions that are fair, reasonable and non-discriminatory within the class of parties that have been afforded an access right.

(4) The recipient 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 paragraph (2); or

(c) any agreement between the parties, including an agreement concerning duties and restrictions imposed by the controller on the recipient under Article 8.

The recipient may not utilize that data in a way that harms the legitimate interests of the original holder more than is inherent in the purpose for which the right was afforded.

## 3.4. Tools for data sharing: smart contracts

In the Public Consultation, the European Commission poses a number of questions on the role which smart contracts might play in the sharing of data by way of automated data transfers. The term "smart contracts" refers to self-executing computer programmes, usually within a system making use of blockchain and Distributed Ledger Technology (DLT). They do not have to be "contracts" within the legal meaning of the term, although they can be employed also in a contractual context.

Such self-executing computer programmes may in fact be employed already for contract conclusion, e.g. a supplier of data (such as an owner of an IoT device) makes an offer to the public to share IoT data, which can be accepted by transferring a certain amount in cryptocurrencies to the supplier's account, which then automatically triggers supply of certain IoT data to the payor. This can facilitate the management of large numbers of data access requests and allow for cost-efficient monetarisation of data by data producers. Needless to say, very little information can be conveyed on-chain, e.g. details about what the recipient of the data may or may not do with the data, choice of applicable law, etc., are difficult to agree upon on-chain. This is why standardised conditions of data access and use (e.g. of the type we see in IP law, such as Creative Commons licences) would be extremely beneficial as mere reference to a standard would be sufficient, which would be machine-readable and suitable for execution by machines.

More often, such self-executing computer programmes are employed for contract execution or beyond any contractual context, e.g. withdrawal of consent by a supplier of data (such as the owner

of an IoT device who has given consent under e-privacy legislation) may automatically trigger certain reactions of the system. However, it must be borne in mind that the benefits of blockchain and DLT are present mainly when all the relevant activities occur on-chain. Events in the off-chain world (such as withdrawal of consent) need to make it onto the chain, and smart contracts can produce effects in the off-chain world (such as deletion of data) only by way of interfaces (often called "oracles") with other digital and non-digital technology. Given that data transfer and use mostly occur off-chain, smart contracts as such would not provide absolute protection against the data recipient breaching the terms under which data were made available, or absolute protection against the data recipient retaining a copy of the data deletion of which has been requested. So either rather sophisticated technology is used that makes sure data access and use fully occurs on-chain, or the recipient gets mere access to the data on the supplier's device or in another secure space, and data processing activities are monitored and logged, allowing derived data to be ported only when it fulfils certain conditions (such as anonymization). Different technology would be required to achieve this, but the last step, i.e. automatic release of derived data, could again be effectuated by smart contracts.

On balance, smart contract technology seems to be a suitable tool for allowing the cost-efficient monetarisation of IoT data by data producers (such as the owners of IoT devices) in a high number of standardised low-value transactions, or the altruistic sharing of IoT data on a large scale. Standardisation of conditions and protocols is essential for making this a truly efficient tool. It is to be stressed, however, that smart contracts as such do not change what is happening in the off-chain world, i.e. the full benefits for data management, including ensuring compliance with standardised conditions under which data transfers were made, can only be achieved with the help of additional technology, some of which may have to be very sophisticated.

## 3.5. Clarifying rights on non-personal Internet-of-Things (IoT) data stemming from professional use

In the Public Consultation, the European Commission is posing questions about rights on non-personal IoT data stemming from professional use. The Authors would like to point out that, in their view, this is an aspect mainly to be conceptualised and addressed within the wider framework of unfairness tests for data related contracts and commercial practices, which is why the Authors primarily refer to the recommendations made concerning "unequal bargaining power scenarios" above at 3.2.2

### 3.5.1. Applicability of the horizontal measures on B2B data sharing

The use of IoT products is a typical scenario, where data is generated by multiple actors many of whom have an interest in using the co-generated data. However, the data is often controlled exclusively by one of the parties who have contributed to the generation of the data (usually the manufacturer of the IoT device, or a third party cooperating with that manufacturer), which gives that party the factual power to decide whether and under what conditions other parties may access the data. Whether or not there is a contract between the parties, and whether or not the problem has its roots more in a contractual term or in a commercial practice, any such arrangements should be subject to an unfairness test (for details see above at 3.2.2).

The Authors wish to stress in this context that it is not advisable to limit measures in the IoT environment to non-personal data, as seems to be suggested in the Public Consultation. In light of the fact that the concept of personal data is extremely broad and the fact that the GDPR also applies to non-personal data if 'inextricably linked' to personal data,[26] most scenarios would not be properly addressed by measures that include only non-personal data. Instead, and as suggested under 3.2.2, a legal framework should be established that also applies to personal data but that provides for strong protection measures, in particular for the rights of data subjects (e.g. sharing data only with trusted third parties or fully anonymising data).

### 3.5.2. Additional transparency obligations

The horizontal measures for B2B data sharing could be complemented by an IoT specific transparency obligation. Often, end users will not exactly know what kind of data is generated by the IoT product they own and operate, and the same holds true for parties interested in using the data. Without the relevant information, the potential of IoT data may remain untapped

Transparency obligations that improve the situation

[26] COM(2019) 250 final, 7; SWD(2017) 304 final, 3.

of the person seeking access vis-à-vis the data controller are already known from the Platform to Business (P2B) Regulation[27]. According to Article 9, platform providers must include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the platform services concerned or which are generated through the provision of those services. Similar transparency obligations could be introduced for the manufacturers of IoT devices, with appropriate exceptions, in particular for MSMEs so as not to create too much additional red tape.

**CHAPTER V: Duties of Manufacturers**

….

Article 15: Transparency obligations with regard to IoT data

(1) The manufacturer of a product or service that generates data while being used must provide information in a clear and transparent manner and by means that are easily accessible both to the users of the product and services and to the public, with regard to

a) the types of data generated by the product or service and any technical specifications of this data to the extent typically relevant for data re-use;

b) the conditions, including any standard licences, under which the user of the product or service may choose to make the data available;

c) the technical means, such as any smart contracts, by which the data may be made available, and how a third party who wishes to re-use the data may access them;

d) ….

(2) The transparency obligations under paragraph (1) do not apply to …

(3) Manufacturers of products and services comply with the obligations under paragraph (1) to provide information in a clear and transparent manner if they use the model in Annex III, duly filled in.

[27] Article 9 of Regulation (EU) 2019/1150.

## 3.6. Improving portability for business users of cloud services

The scenarios outlined above where multiple actors have contributed to the generation of data, which is stored on the servers of one out of several contributing parties, need to be clearly delineated from the situation that companies store their data with a Cloud Service Provider (CSP). In the latter constellation, the data is generated solely by the Cloud Service Customer (CSC) that uses the services of the CSP to store its data. Cloud service contracts usually contain elements of service, leasing and storage contracts to different degrees, depending on the concrete agreement. Where the CSP stores the CSC's data, the parallels to traditional contracts for the storage of tangible goods are more than obvious. The CSC 'hands over' data to the CSP with the mutual intention of the parties to ultimately have the data returned to the CSC. Under traditional storage contracts, the client may request the return of the stored item from the storer at any time even if the contractual storage period has not yet ended. Of course, the agreed price for the storage has to be paid in full.[28] Furthermore, the storer may not use the stored items[29] and has to return them at the end of the contract period or upon termination of the contract.[30]

The legitimate interests of a CSC do not differ from those of a customer in a traditional storage contract. Hence, at any time should the CSC be allowed to retrieve the data that was provided to the CSP. The agreed fee must be paid for the full contract period or until the earliest possible termination date. It would also not be reconcilable with the nature of a storage contract, if the CSP were allowed to use the data provided by the CSC.[31] While returning a tangible item ensures that it cannot be used by the storer, data, due to its non-rivalrous nature, could be copied before it is returned. A functionally equivalent rule for cloud service contracts would therefore be that after the contract has lapsed or is terminated, the CSP has to erase all data provided by the controller and is not allowed to retain any copies of it.[32]

These three ground rules are essential to ensure that CSC do not lose control over their data when transferred to a CSP. Hence, the Authors recommend that they should be made mandatory by law and not left to self-regulation. One feasible option to give these central rules mandatory effect is by drawing up a cloud-specific grey and/or black list that would complement the fairness test and the general grey and/or black list for co-generated data (see 3.2.2.2). It would be, in particular, any terms that prevent the CSC from retrieving the data or allow the CSP to use the data or keep a copy after the contract was terminated would be considered/presumed unfair and non-binding. The rules could draw inspiration from the default rules recommended in Principle 12. In order not to confuse the scenario of co-generated data and the cloud storage scenario it is advisable not to merge the two, but to have a separate unfairness test with separate grey and/or black lists, possibly in a separate Chapter of the Data Act.

Other aspects such as technical measures to facilitate portability between different CSP can be addressed by a self-regulatory regime, such as SWIPO. Self-regulation should, however, be coupled with a certification scheme in order to help potential CSC to identify providers that allow for an easy transition between CSP.

## 3.7. Complementing the portability right under Article 20 GDPR

In the Public Consultation, the European Commission is explaining its plans to tackle lock-in effects and enhance data availability in the IoT setting by enabling owners and long-term users of connected devices to efficiently port the data generated by their connected devices, such as wearables or household appliances. The Commission suggests complementing the existing data portability right under Article 20 GDPR with a technical infrastructure that would enable continuous and real-time portability.

### 3.7.1. Portability for all data generated by the use of an IoT-device

The wording of the Public Consultation and the impact assessment seem to suggest that the Commission envisages an expanded data portability right in the IoT setting only for personal data. However, since the interest of owners and long-term users to port data generated by an IoT device is not limited to personal data, the Authors would strongly recommend that such a right should include all data generated by an IoT device. The traditional argument against introducing portability rights for non-personal data, i.e. that it is unclear to whom such a right should be granted, falls

[28] Article IV.C. – 5:104(1) DCFR.
[29] Article IV.C. – 5:103(2) DCFR.
[30] Article IV.C. – 5:104(1) DCFR.
[31] See Principle 12(2)(d).
[32] See Principle 12(2)(2).

flat in the IoT context, as it is the owner or long-term user of the device that should be able to port the IoT data.

If a data portability right goes beyond Article 20 GDPR anyway, this should be a welcome opportunity to introduce certain improvements. For instance, the data portability right should – in contrast to Article 20 GDPR – also include certain derived data. Another shortcoming of Article 20 GDPR is that it only applies if data is processed based on the consent of the data subject or is necessary for the performance of a contract. This allows controllers to get outside the scope by relying on 'legitimate interests' instead of consent or contract.

If not included in the Data Act itself, an elegant place to address these issues would be the current proposal for an E-Privacy Regulation[33]. This instrument is already designed to particularise and complement the GDPR[34] and deals with 'electronic communication data' generated by using 'terminal equipment', which is defined as equipment directly or indirectly connected to the interface of a public telecommunications network.[35] Since IoT products are per definition connected to the internet, they would qualify as terminal equipment. Furthermore, the E-Privacy Regulation does apply to personal and non-personal data alike, which would fit well with the suggestion of expanding the portability to all data generated by an IoT device.

### 3.7.2. Technical infrastructure requirements for continuous or real-time portability.

While data access regimes in the energy, payment and automotive sector enable a continuous stream of data access, Article 20 GDPR is rather designed as a one-off mechanism. Continuous and real-time access, however, will often be necessary, in particular, to make use of complementary services. The proposal for the Digital Markets Act[36] addresses this issue in Article 6(1)(h), which stipulates that 'a gatekeeper shall provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise'. A similar provision could be introduced for IoT data, in appropriate circumstances.

In addition, the European Commission, together with standardisation bodies, could develop technical standards that would ensure IoT data can be transmitted directly from one controller to another. Without such standards, controllers may refuse direct transfer, as Article 20(2), gives the right to have the personal data transmitted directly from one controller to another only where this is 'technically feasible'. Examples of provisions referring to technical standards for the transfer of data can already be found in connection with the access rights under the Type Approval Regulation[37] or the PSD II.[38]

### 3.7.3. Safeguards for the protection of end-users and SMEs

While data portability is a tool that can address both lock-ins and enhance the free flow of data, it can also solidify competitive imbalances in the data economy and harm end-users and SMEs. By exercising the right to data portability, other companies than the initial data holder get access to the data which they might not have obtained otherwise. Companies therefore have an interest to actively facilitate the exercise of the right to data portability in order to ensure it is used to their advantage. This may lead to a situation where the right to data portability is not exercised on the initiative of the rights holder but on that of the company benefitting from the right. Companies providing services or products that are used and relied on by a large number of users will be particularly successful in this endeavour as they reach out to a large number of parties and have the technical means in place to allow for seamless and easy porting on a large scale. For instance, the provider of popular navigation services could, where a user searches the way for a particular location, request real-time porting of the user's mobility data held by the car manufacturer or public transport companies with one simple click. Possibly, even mandates to exercise portability rights on another's behalf may be included in the respective standard terms. SMEs that seek to enter the market with innovative services or products, on the other hand, are not yet in a contractual relationship with the rights holder and would therefore not benefit from the data portability right to the same extent as market incumbents. To mitigate the anti-competitive and

[33] COM(2017) 10 final. The current proposal (ST 6087/2021 INIT) is currently in the trilogue.
[34] See Article 1(3) Com(2017) 10 final.
[35] See Article 1(1)(a) Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment OJ L 200(/162, 20.
[36] COM(2020) 842 final.
[37] See Article 61(2) Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers and, and of systems, components and separate technical units intended for such vehicles, OJ L 2018/151, p. 1.
[38] Article 98(1)(d)Directive (EU) 2015/2366 on payment services in the internal market, OJ L 2015/337, p. 35.

privacy-invasive effects of horizontal portability rights sufficient safeguards need to be in place.

The legislative measures should, inter alia, clarify that the requirements for consenting under the GDPR[39] and the future E-Privacy Regulation[40] also apply to the right to data portability in order to protect owners of IoT devices from exercising their right to portability without their knowledge. For example, the request to port data should only be valid if freely given, specific, informed, unambiguous and the owner of the IoT device should be able to withdraw the request at any time.[41]

Intermediaries (or data sharing services in the terminology of the proposal for a Data Governance Act (DGA)[42]) that exercise the right to portability on behalf of the rights holder and technical measures, such as so-called privacy management tools (PMT), will need to play an important role in ensuring that the portability right is exercised in the interest of the rights holder and not those of dominant market players. For example, PMTs could provide an interface that lists the portability decisions right holders have, gives information about the data recipients as well as the purposes for which the ported data is used, and allows for an easy withdrawal of the portability request. Of course, it needs to be ensured that such tools and intermediaries adhere to strict principles of privacy and not themselves turn into large data leeches, exploiting the data they are supposed to protect. With the DGA a legal framework that aims at ensuring the trustworthiness of the data sharing services is already in the pipeline.

Generally speaking, for reasons stated above, the Authors wish to express a degree of scepticism vis-à-vis portability obligations that are the same irrespective of the size of the supplying and the receiving businesses. Instead, the Commission could consider introducing stricter portability obligations for powerful companies than for market entrants and smaller players. An asymmetric data portability obligation has recently been proposed by the Digital Markets Act. Article the 6(h) provides a real time portability right only against gatekeepers and can therefore only benefit non-gatekeeping companies. The Authors welcome this approach and believe it should more generally guide the introduction of more far-reaching portability rights.

## 3.8. Revision of the Trade Secrets Directive

It has already been pointed out under 3.2.1.3 that actors in the data economy may be discouraged from entering into data transactions due to a lack of legal protection against illegitimate data activities by third parties. Recipients may disclose data to third parties contrary to contractual agreements, or a malicious actor may overcome security measures of the recipient and 'steal' the data. Where data does not fall within the scope of legal regimes, such as data protection, IP or trade secrets law, the data holder's protection is rather uncertain, as it depends on national tort law, which may differ significantly. One option to address this issue would be to set out specific rules that protect data against unlawful acquisition, use and disclosure outside contractual relationships. For data that is considered a trade secret such a regime already exists under the Trade Secrets Directive. While the trade secret protection cannot simply be expanded to all data, the Directive's general aim and underlying concepts are similar to those that should also guide the rules on third party aspects of data activities. Therefore, the Authors have suggested that mandatory rules on the protection of data holders against unlawful data activities and the effects of data processing activities on third party rights could be included in a separate chapter of the Trade Secrets Directive. For suggestions on how such provisions could look like, reference can be made to 3.2.1.3.

[39] See Article 4(11), Article 7 and Article 8 GDPR.
[40] See Article 4a(1) ST 6087/2021 INIT which refers to the provisions of the GDPR.
[41] Article 4(11) GDPR and Article 7(3) GDPR.
[42] COM(2020) 767 final.

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9504549-8-7