Response to the public consultation on "A European strategy for data" COM(2020) 66 final

John Thomas, Lord Thomas of Cwmgiedd, Essex Court Chambers, formerly Lord Chief Justice of England and Wales, The United Kingdom, LordThomas@essexcourt.com

Christiane Wendehorst, Professor of Law at the University of Vienna, Austria, Christiane.Wendehorst@univie.ac.at

European Chair and European Reporter of the transatlantic project "Principles for a Data Economy" conducted jointly by the American Law Institute and the European Law Institute

Project assistant: Dr. Sebastian Schwamberger, University of Vienna

---

The present response does not reflect the official view of the European Law Institute or of the University of Vienna or of any other body the authors may be associated with.

---

1. Introduction

The authors are part of a joint project of the European Law Institute (ELI)[1] and the American Law Institute (ALI).[2] The "**ALI-ELI Principles for a Data Economy**" 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. Currently the Reporters of the project Neil Cohen (ALI) and Christiane Wendehorst (ELI) are working on the finalization of Preliminary Draft No. 4, which contains the following six Parts:

(I) General Provisions
(II) Data Contracts
(III) Data Rights
(IV) Data as an Asset
(V) Third Party Aspects of Data Transactions
(VI) Multi-State Issues

The authors welcome the opportunity to respond to the public consultation of the European Commission. To start with, they wish to express their **full support of all four pillars of the strategy**, i.e.

A. A cross-sectoral governance framework for data access and use;
B. Enablers: Investments in data and strengthening Europe's capabilities and infrastructures;
C. Competences: Empowering individuals, investing in skills and in SMEs; and
D. Common European data spaces in strategic sectors and domains of public interest

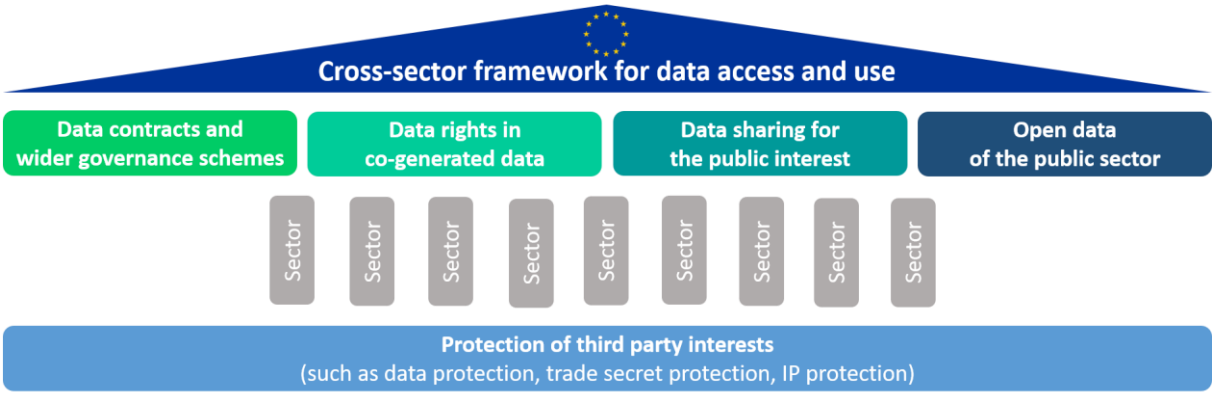
[1] https://www.europeanlawinstitute.eu/principles-for-a-data-economy/.
[2] http://www.thealiadviser.org/data-economy/.

Against the backdrop of the subject matter addressed by the "Principles for a Data Economy" the authors will **focus their response on pillar A**, i.e. on the cross-sectoral governance framework for data access and use, and within pillar A on the legal aspects.

2. Five cross-sector frameworks for data access and use

The authors **strongly support the cross-sectoral approach** taken by the European Commission in the Data Strategy. While a purely sectoral approach may appear to be less challenging and ambitious in several respects, it might result in a patchwork of widely diverging solutions that are not based on a consistent set of principles, but rather on the vicissitudes of policymaking and legislative procedures in the various sectors. The authors believe that sector-specific measures will definitely be necessary. However, the development and negotiation of sector-specific standards would greatly benefit from the coordinating and catalyzing function of a cross-sectoral framework.

In the eyes of the authors, the relationship between cross-sector ('horizontal') and sector-specific ('vertical') measures can be visualised as follows:



Strictly speaking, there may be a need not for one single cross-sector framework, but rather for **four different, more or less 'horizontal' frameworks**, namely:

1. Data contracts and wider governance schemes (cf. ALI-ELI Principles Part II);
2. Data rights in co-generated data (cf. ALI-ELI Principles Part III A and B);
3. Data sharing for the public interest (cf. HLEG B2G Data Sharing; ALI-ELI Principles Part III C);
4. Open data of the public sector (cf. Directive (EU) 2019/1024).

These four frameworks have in common that they address different schemes within which sharing of data occurs. Given that sharing of data may affect not only the parties to the transaction, but also protected third parties there is a range of cross-sector protective regimes, such as data protection, trade secret protection, and IP protection, but also the protection of upstream suppliers. This leads to a truly 'horizontal' fifth cross-sector framework, dealing with the effect of third party rights on data access and use:

5. Protection of third party interests (cf. ALI-ELI Principles Part V).

The authors strongly recommend **not to create different frameworks for the sharing of personal data and the sharing of non-personal data** in the first place but rather to treat data protection as a cross-sectoral element that may have implications for, and impose limitations on, data sharing.

3. Need for action at EU level

The authors believe that there is need for EU action with regard to all of the five cross-sectoral frameworks just mentioned, albeit certainly not to the same extent.

3.1. Data contracts and wider governance schemes

As far as data contracts are concerned (cf. ALI-ELI Principles Part II), it may be sufficient that the EU develop and make available, e.g. through its Support Centre for Data Sharing (SCDS), a series of **model agreements**. They would be beneficial in order to facilitate data sharing also for SMEs and less sophisticated players in the data economy, e.g. companies whose primary business is not in the data field. The Reporters and Chairs of the "Principles for a Data Economy" project are happy to assist in the process, if necessary.

The EU may also consider going one step further, i.e. into the direction of default rules and/or blacklisted unfair terms for B2B contracts. In this context, the authors wish to draw attention to the issue of **'sales approach' vs. 'license approach'**. In practice, a 'license approach' has become the predominant approach, i.e. the parties to a data transaction treat data as if it were protected by IP rights. Accordingly, they tend to call their contracts a 'license', giving rise to limited 'data utilization rights', and any data utilization beyond what is stated in the contract is considered to amount to breach. The ALI-ELI Principles have rather opted for a 'sales approach', based on the principle of 'free by default', i.e. the recipient of data may normally use the data "*for any lawful purpose and in any way that does not infringe the rights of the supplier or third parties …"* unless the parties agree otherwise. The 'license approach' is restricted to closed data platforms and some other cases.

The EU might also wish to consider more far-reaching steps with regard to **data marketplaces** and **data trusts**. In both cases, an approach that goes far beyond contract law and in the direction of comprehensive data governance schemes (including, inter alia, a range of objective standards and certification criteria) would be preferable. The authors would like to stress that it is in particular the development of data trust schemes that might prove to be a **precondition for European data spaces and enhanced data portability to achieve the desired effects**. Without such intermediary schemes in place, there is otherwise a danger that these measures predominantly serve to still increase the market power of some few dominant players in the data economy that do not need such intermediaries.

3.2. Data rights in co-generated data

The concept of data rights in co-generated data (Part III of the ALI-ELI Principles) has been developed by the ELI and ALI and has gained far-reaching acceptance since then. Amongst others it has been adopted, as an ethical framework underlying data access and use in the data society, by the German Data Ethics Commission in its 2019 opinion.[3] Part III of the ALI-ELI Principles may be taken into account by courts when interpreting contracts and assessing the fairness of contractual clauses as far as this is possible under the applicable national law. However, there may be a need for more far-reaching implementation and for more robust enforcement of rights in co-generated data, which would require legislative action at EU level.

While co-generation of personal data is dealt with by the GDPR, co-generation of non-personal data has become a major issue, in particular with the rise of the IoT in industrial settings. The authors applaud the European Commission for having dropped, as it seems, plans to introduce a 'data producer's right' as an exclusive 'data ownership' right. However, the authors believe that it is of the

[3] Opinion of the German Data Ethics Commission, 2019, p. 85 ff. https://datenethikkommission.de/.

essence to recognise certain non-exclusive rights which a party that has contributed to the generation of data may have against the controller of such data, in particular access and porting rights. The authors therefore **strongly recommend that the Data Act 2021 include a cross-sectoral framework addressing rights in co-generated data**, in particular in the IoT (for a mor in-depth explanation see point 4 below).

3.3. Data sharing for the public interest

The ALI-ELI Principles will deal with data sharing for the public interest in Chapter C of Part III. The authors will refrain from elaborating on this in their response to the consultation, both because Chapter C is still being developed and because there exists the very comprehensive report by the High-Level Expert Group on Business-to-Government (B2G) Data Sharing.

However, the authors would like to point out that B2G data sharing is just one part of this cross-sectoral framework, and that there exists also B2B data sharing that is based predominantly on notions of public interest (e.g. the desire to reduce unnecessary testing on animals, cf. REACH). Also the delineation between data rights in co-generated data and B2B data sharing for the public interest is sometimes not clear-cut, but blurred. The authors are wondering whether the notion of **'empowering individuals'** with regard to their co-generated data (see Data Strategy p. 20) might here or there be confused with **what is really fostering data sharing for the public interest**. This concerns, in particular, the further strengthening of data portability rights beyond what the party exercising the right needs for switching providers or for a similar purpose in that party's clear own interest. Where data subjects exercise their portability rights under Article 20 GDPR (or where someone exercises a new, extended portability right) in the predominant interest of a third party or of research in general ('data donation') in order to make more data available for the European data economy this amounts to **C2B or C2G data sharing for the public interest.** While the authors do not wish to be understood as saying this should not happen, they wish to stress that the underlying principles and applicable tests are not those for co-generated data (ALI-ELI Principles, Part III, Chapter B), but those for data sharing for the public interest (Part III, Chapter C). They also wish to re-iterate (see already 3.1) that, in order for enhanced portability rights to achieve the desired aims, appropriate data governance structures need to be put in place, including **reliable data trust schemes**.[4]

3.4. Open data of the public sector

Given that the Open Data Directive (EU) 2019/1024 has been passed only recently, the authors do not currently see a need for much EU action in this area. However, they welcome the European Commission's plans for a **delegated act** on high value data sets. In addition, they wish to point out that the uncertainty with regard to the required level of protection of third parties (in particular data protection) may prove to be a major obstacle for open data becoming fully effective and that, for unleashing open data's full potential, it could be advisable to develop **security standards, model license agreements and similar 'safe harbour tools'** for the public sector. These could also be used to mitigate potential adverse effects of open data concepts, such as public sector data being used to the detriment of the public interest, and/or the taxpayer having to pay twice.[5] The ALI-ELI Principles will not be dealing with open data of the public sector, though.

[4] German Data Ethics Commission (n. 3), p. 133 ff.

[5] For details see German Data Ethics Commission (n. 3), p. 150.

3.5. Protection of third parties

Any cross-sectoral framework for data access and use needs to provide for adequate and effective mechanisms for the protection of third parties.

3.5.1. Better trade secret protection in the IoT

The Trade Secrets Directive, although an excellent piece of legislation in many respects, is not well adjusted to the IoT, and specifically in industrial settings. Amongst others, it is impossible for the businesses operating IoT devices to take reasonable steps to keep information secret where the information is only derived or deferred from IoT data collected in a cloud, in particular as providers etc collecting the data may have more information about the business than the business itself. Also, the role of consent for trade secret protection is unclear as businesses operating IoT devices tend to click 'I agree' at various instances during the configuration of a device, or accept far reaching standard terms in a contract. It may even sometimes be unclear who is the legitimate holder of a trade secret. This may call for **adjustments in the Trade Secret Directive** or, alternatively, for **protection under a regime for rights in co-generated data** (see Case No. 2 under 4.3 below).

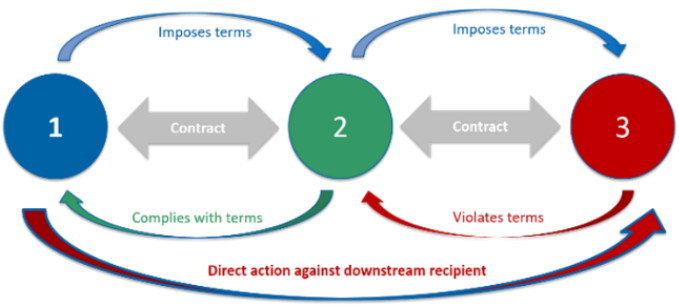
3.5.2. Avoiding or reducing chilling effects

Taken together, data protection, trade secret protection and IP protection, may have a **chilling effect on data sharing** because of the uncertainties that come with these protective regimes, in particular in the case of large and mixed data pools. Considering the very broad notion of 'personal data', the very broad and fuzzy scope of sui generis database protection, and remaining problems with text and data mining (TDM), these uncertainties may seriously impair data sharing activities. The ALI-ELI Principles do not address this because of an agreement between the ALI and the ELI not to deal directly with data protection, trade secrets and IP, but rather to take restrictions under these regimes as given. However the authors wish to point out that the EU might improve the situation through a **combination of de minimis rules, fair use exceptions and liability privileges based on a 'notice and take out' model**, providing certainty to parties in the data economy in cases where interests of third parties are hardly affected and where the parties to a data transaction did not have notice (e.g. of the fact that there were some few pseudonymised personal data in a large data set required for training AI).

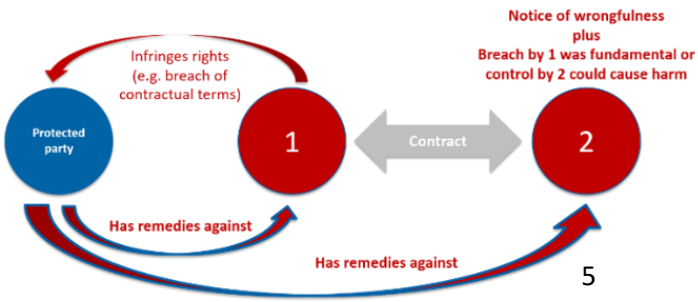
3.5.3. Downstream third party effects of contractual limitations

Part V of the ALI-ELI Principles includes guidance on how third party protection beyond data protection, trade secret protection and IP protection might look like. It does so mainly with regard to (i) contractual limitations on data utilisation and (ii) illegality of the way data were originally obtained (e.g. where data were obtained by way of hacking). The protective regime developed in Part V of the Principles, which has been inspired by the Trade Secrets Directive, has been favourably received, inter alia, at several meetings hosted by UNCITRAL. It includes ways of making a **downstream recipient of data directly liable** vis-à-vis a protected party upstream. This may provide data suppliers with the certainty and degree of control they need, thus encouraging the sharing of data, without stifling the data economy (as would probably be the case with exclusive ownership rights in data).

'Leapfrogging' with middleman acting rightfully



'Leapfrogging' with middleman acting wrongfully



4. Special focus: Data rights in co-generated data

The authors support the possible adoption of a Data Act 2021, which would also address issues related to usage rights for co-generated data (such as IoT data in industrial settings). The ALI and ELI have developed the concept of rights in co-generated data, and have coined the term.

4.1. What are data rights?

Data rights are legally protected interests that arise from the very nature of data as information recorded in any form or medium. Data is a non-rivalrous resource, which may be used by many different parties for many different purposes at the same time, and to the generation of which many parties may have contributed in many different ways These attributes are taken into account when recommending the recognition of a new data-specific class of rights, which the ALI-ELI Principles call 'data rights.' Rights of this nature are being recognized to an increasing extent in data-specific legislation and case law worldwide. They are not purely contractual, as they may exist between parties without any contractual link, and they do not reflect ownership notions in the traditional sense because traditional notions of ownership do not work well with resources of a non-rivalrous nature. The data rights dealt with under the ALI-ELI Principles fulfil functions similar to those fulfilled by ownership with regard to traditional rivalrous assets. However, the notion of data rights recommended by the ALI-ELI Principles is not identical to that of ownership rights. While the right to control a resource as against any person who has a lesser right is central to ownership in the classical sense, these Principles take the position that the right to have *non-exclusive* access to data or to port data is central to any equivalent of the concept of ownership in the data economy, not least because the overall welfare is normally increased where more than one person can exploit the data for economic purposes. The ALI-ELI Principles set out a non-exclusive list of four basis data rights:

(1) Access or Porting of co-generated data

(2) Desistance from the use of co-generated data

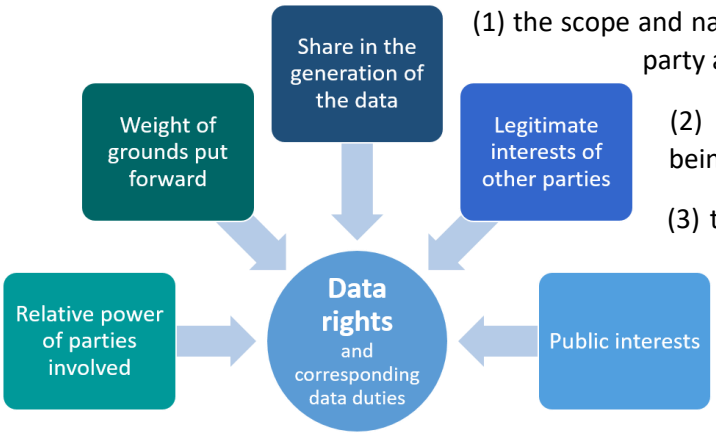
(3) Correction of co-generated data

(4) Economic share in profits derived from co-generated data

4.2. Who should have a data right and against whom?

Data Rights with regard to co-generated data are based on the fact that data is usually generated by the contribution of various parties, e.g. by being the subject of the information, or the owner or long-term user of the object of the information, by performing an activity by which the data were generated, or by having rights in a product or service that has contributed to the generation of data. Co-generation is not only a matter of Yes or No, but what is decisive is the extent to which a party has contributed to the generation of particular data. Contributions of a party that are insignificant in the circumstances do not lead to data being considered as co-generated by that party.

Having contributed to the generation of the data can justify the recognition of a data right which can be enforced against the controller of the co-generated data. The controller is the person that is in a position to access the data and determine the purposes and means of its processing. But having contributed to the generation of the data is only one out of five factors that have to be considered when determining rights in co-generated data:



(1) the scope and nature of the contribution to data generation by the party asserting a data right;

(2) the weight of that party's legitimate interest in being granted said right;

(3) the weight of any possibly conflicting interests on the part of the other party or of third parties, taking into account any potential compensation arrangements;

(4) the interests of the general public;

(5) the balance of power between the party asserting the data right and the other party.

The question of whether or not a data right with regard to co-generated should be recognised is inextricably linked with the question of how this right should granted, i.e. what are the modalities with regard to formats, timing and the like, and whether access must be provided for free or in return for appropriate remuneration. In order to define the modalities, courts and legislators will in particular have to consider the data right that is in question, the type and weight of the parties' respective shares in the generation of the data as well as the efforts required for complying with the right. The five general factors that determine data rights in co-generated data will play an important role.

4.3. Case studies

Case No. 1: Access to data by the supplier of a component

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 are 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). All of this data is sent to and stored on cloud servers controlled by D under a contract with C. Access to that data would enable T to improve tire performance. Accordingly, T seeks access to the data concerning its tires. C and D decline to grant such access because D is considering developing smart services utilizing the data and does not want anyone else to develop the same services, and 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 by T (together with C and E and possibly other parties), albeit to a lesser extent than by C or E. Quality monitoring or improvement by a supplier in a value chain is one of the standard grounds for claiming access to or porting of co-generated data, when monitoring and improvement it is in line with duties of that supplier within the value chain and the controller of the data can be expected to have foreseen and accepted this role. There is thus a strong legitimate ground for T to request access to the data relating to the tires, but legitimate interests of the controller or third parties (such as E) are equally a factor to be taken into account, as are the relative bargaining power and public interests. This could mean in the individual case that a data right vis-à-vis D is afforded only with appropriate restrictions such as anonymization or, depending on the circumstances, access via a trusted third party.

Case No. 2: Database for investors in farmland

Farm corporation F buys a 'smart' tractor which has been manufactured by manufacturer M and which provides various precision farming services, including weather forecasts, soil analyses and targeted recommendations concerning the use of particular fertilizers and insecticides. M also uses the soil and weather data collected by the tractor to create a database that could be sold to 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.

Among the data rights dealt with by the Principles is the right to require a controller of co-generated data, such as M, to desist from particular data uses. Without any doubt, F has had a huge share in the generation of the data collected by M, so F might have a right to require that M refrain from using the data relating to F's farmland in such a way. Grounds that may give rise to a party's right to require that the controller desist from using co-generated data in a particular way include the fact that the use is likely to cause significant harm to that party. However, that alone is normally not sufficient, and further elements are required. For instance, the party must have contributed to the generation of the data for another purpose that is inconsistent with the contested use, and that party could not reasonably have been expected to contribute to the generation of the data if it had foreseen the harm that would result.

The situation in the Case Study could cause significant harm to F because potential buyers might have better information about the soil quality than F itself, so using F's data for this purpose could harm F's interests in the event of future negotiations about F's land. F has contributed to the generation of the data for an entirely different purpose (ie in order to benefit from precision farming services), disclosing the data to buyers of land is entirely inconsistent with that purpose, and it is highly likely that F would not have agreed to produce the data if F had known about how T would make use of the data.

4.4. How could data rights be implemented in the Data Act 2021?

As to the way rights in co-generated data could be implemented in the Data Act 2021 there are several different options, and a lot depends on the scope and structure of the Act and some bigger strategic decisions to be taken by the European legislator.

Where the party exercising a right in co-generated data and the controller of co-generated data have a contract, the most obvious implementation would be via contract law, either by way of

- default contract rules combined with 'soft' unfair terms control (including for B2B); or
- blacklisted unfair contract terms (including/predominantly for B2B contracts).

However, there are many constellations where there is no contract between the parties involved, such as in the relationship between an end user and a manufacturer, or the supplier of a component and a third party service provider (see Case No. 1 under 4.3 above). It is therefore of the essence that implementation of rights in co-generated data in a Data Act 2021 is broader in scope, extending these rights to relationships that are not contractual in nature. It may therefore be necessary to introduce **a new statutory regime of data rights**, either by way of

- opt-out rules combined with 'soft' unfair contract terms control (including for B2B); or
- blacklisted unfair practices (including/predominantly for B2B).