B2 – Analytical report on EU law applicable to sharing of non-personal data

Support Centre for data sharing

DG CONNECT

SMART 2018/1009

24 January 2020

V2.0

Table of Contents

Executive Summary

This analytical report is drafted by the Support Centre for Data Sharing (SCDS), an initiative funded by the European Commission to further support the development of the Digital Single Market. More specifically, the SCDS' objective is to facilitate data sharing, i.e. transactions in which data held by the public or private sector are made available to other organisations (public or private) or citizens for use and re-use. Data sharing can happen in exchange for payment (or other reward) or for free, and (re-)use may be entirely free or conditional. The success of data sharing depends on practices, technology, cultural elements and legal frameworks that are relevant to sharing any kind of information digitally, between individuals or organisations.

This report is part of a range of analytical reports which will be delivered by the SCDS during the course of its operations. This report focuses in particular on a thorough analysis of EU legislation applicable to the sharing of non-personal data, and aims to provide a structured overview of all the relevant European instruments relevant within this field.

As a first step in this objective, our team identified the EU applicable acquis - accumulated legislation, legal acts, and court decisions which constitute the body of European Union law that affect data sharing possibilities and practices. This acquis was thereafter further analysed and summarised. As a third and last step, our team summarised the general trends in the EU, including the identification of cross cutting challenges, and potential resolution strategies and identified best practices or interpretative guidance. The outcomes of this analysis are contained in this report, which will be expanded through future updates.

Based on the analysis in this report, the principal finding is that, while the encouragement of data sharing through legislative intervention is clearly and structurally on the rise, the drivers behind this push differ from topic to topic. Key recurring drivers include encouraging transparency, consumer protection, stimulating fair competition, supporting innovation and research, increasing security, and protection of fundamental rights. There is however not always a clear statement of the driver(s) behind specific legislative interventions. As a result, regulatory approaches are not always consistent from subject matter to subject matter, which implies additional effort for aspiring users: it would be naïve and incorrect to assume that legislation universally favours unconditional availability and use of data; a case by case assessment is always required.

Common trends do emerge in recent legislative initiatives. These include a specific focus on dynamic data (i.e. information that is subject to frequent or real-time updates, and is therefore increasingly made available via APIs), on enabling/facilitating scientific research (including AI and big data), and on ensuring adequate security measures. The assessment also shows that not all legislation uniformly favours data sharing: leaving aside data protection law as being out of scope of the present report, legislation focusing on confidentiality and intellectual property rights emphasises the protection of lawful rights holders, while also harmonising some exceptions for lawful recipients of the data; this can impact data sharing.

To improve consistency in policy making, it would be beneficial to explicitly define high level strategic objectives for data sharing in the EU in general, and to derive the implications (and thus required legislative intervention) for each regulatory initiative, taking into account with other legitimate policy objectives, including the protection of confidentiality and intellectual property rights.

1 Introduction

The objective of this report is to assist the European Commission in developing guidance on the legal acquis at EU level that is relevant for drafting contractual license agreements on sharing of non-personal data (i.e. data using agreements). This report analyses legislation insofar as harmonised at EU level, as well as relevant jurisprudence at national and EU level interpreting key concepts of these instruments. It is not intended to comprehensively analyse legal problems to data sharing in the EU, nor to provide solutions from a legal or policy perspective. It is intended to offer a representative overview of legal frameworks that can impact data sharing practices and licensing options. The report builds on available material and shall be updated regularly during the course of the project.

The legal conditions for the sharing and re-use of personal data – or to use the parlance of data protection law: making personal data available to third parties to enable processing for different purposes than those for which it was originally collected – are relatively clearly regulated by the General Data Protection Regulation 2016/679 (GDPR).

Conversely, the law and legal practice for non-personal data is much less clear. Non-personal data is regulated on an ad hoc basis in the EU. Arguably, an explanation may be the assumption that non-personal data can be freely shared, and thus that only exceptions need to be regulated. As a result, the legislation by necessity focuses on these exceptions, which may create an appearance of fragmentation. Some of this data will be subject to more general provisions, such as those of Open Data Directive of 20 June 2019 in case of public sector information, and the Regulation on the free flow of non-personal data of 14 November 2018. Additionally, some of the data will be subject to sector-specific rules, such as the PSD2 Directive of 25 November 2015 in case of the financial transaction data, and the Clinical Trial Regulation of 16 April 2014 in case of clinical trial data. None the less, this is far from the complete picture, and there is a wide body of EU law that can affect the terms of data sharing.

The process for drafting such an analytical report is composed of three steps:

- **Step 1: The identification of the relevant legal acquis at EU level;**
- **Step 2: The analysis of the selected acquis and;**
- **Step 3: A summary of the general trends.**

Step 1: Identification of the relevant acquis - accumulated legislation, legal acts, and court decisions which constitute the body of European Union law.

The identification process is done in coordination with the European Commission. The identified legal frameworks include general legal frameworks, such as the Open Data Directive and the Free Flow of Non-Personal Data Regulation; but also sector specific frameworks, such as the PSD2 Directive for financial transaction data, the Clinical Trial Regulation for clinical trial data, the INSPIRE Directive for geographic data, the RMI Regulation for vehicle repair and maintenance information, the European

Electronic Communication Code for electronic communications, the new Energy Framework for energy consumption data, etc. Relevant legislation is selected through desk research on key policy areas which are data driven, and can be expanded throughout the project when new relevant legislation is identified or emergeds. A more comprehensive overview is provided in the sections below.

Step 2: Analysis of the selected acquis.

The identified EU instruments from step 1 are used as input for step 2, which consists of an analysis of the selected acquis. This implies a full description of at least the following elements:

- **Which data** is targeted by the legislation;
- What the **obligations or requirements** of the legislation are;
- **Who is affected** both as a data source and as a data user;
- **What the potential challenges and pitfalls are,** including any topics which are subject to national implementation or policy choices. Relevant jurisprudence at national and EU level will be identified as well. It should build on available material and be updated regularly during the course of the contract.

Step 3: Summary of the general trends, including identification of cross cutting challenges, and potential resolution strategies and any identified best practices or interpretative guidance.

As a conclusion, this report highlights any identified red threads between the examined regulatory texts, and comment on potential quick wins and longer-term policy choices that can address existing challenges.

1.1 Purpose of this document

This document aims to provide an analytical report on the EU legislation applicable to sharing of non-personal data, by means of a structured and systemised overview.

The information on the relevant EU acquis applicable to the sharing of non-personal data is collected principally through desk research for each of the targeted sectors, supported by existing studies that have already been conducted at the EU level on this topic. No systemic review of national implementing law is foreseen, but where available implementing legislation and policies will be consulted, in particular to identify national constraints and obligations, or best practice guidelines.

1.2 Structure and content of this document

The report is structured as follows:

1. Introduction – provision of the general context, objectives and used methodology
2. Identification of the EU acquis applicable to data sharing
3. Analysis of the EU acquis applicable to data sharing
4. Summary of the general trends
5. Conclusion

Figure 1 Structure of the document

1.3 Next steps

While this deliverable is a static document and submitted in month 20 of the project, it is understood that the content of this deliverable will be updated throughout the course of the project due to the feedback the team will receive from stakeholders.

2 Identification of the EU acquis applicable to data sharing

2.1 Vision and general approach

Despite the importance of data sharing in the development of the information society and in the creation of new and innovative services, there is currently no clear perspective on the legislation in relation to the sharing of non-personal data. Knowledge on this topic is unclear, complex and fragmented. As such, it is hard to identify common patterns, commons strategies and common challenges, or to define fact-based policies to address potential challenges. The present report provides inputs to address this problem.

This section of the deliverable aims to provide a short overview of the EU acquis applicable to the sharing of non-personal data. In the present section, the legislation will merely be listed, along with a short statement on the type of data targeted by the legislation and its relevance to data sharing.

As will be shown below, the sharing of non-personal data may be subject to so-called general and horizontal legislation – i.e. legislation which is not linked to a specific industry or field of activity – or to sector-specific instruments. The impact of the former category is potentially broader, or at least harder to cleanly demarcate, than that of the former.

Consequently, a distinction will be made between general legal frameworks on the one hand and sector-specific legal frameworks on the other. Key examples of legislation are provided below.

Section 3 below will provide a more comprehensive description of the legal frameworks, in each case covering the following topics:

- **Short summary**: a statement of the general objectives of the legislation, without focusing specifically on the data sharing aspects;
- **Objectives in relation to data sharing**: a statement of the legislation's intended goals in relation to data sharing;
- **Parties targeted or affected**: a statement identifying which parties are required to share data, and with whom;
- **Data targeted or affected**: a statement identifying the data to be shared or otherwise targeted;
- **Short assessment of its impact**: a statement of observed and likely impacts, including any known potential indirect consequences

2.2 General and horizontal legislation

This section provides an overview of certain key EU legislative texts that touch upon aspects of data sharing in general (i.e. without focusing on any particular sector or industry). While some of these legislative frameworks at first sight do not refer to sharing of non-personal data, they are none the less important due to their potential impact on data sharing in the EU, as will be further explained in the sections below.

The present version of this report includes assessments of:

- The GDPR, targeting personal data[1];
- Competition Law – TFEU[2], mainly its impact on data sharing decisions in markets where there is a risk of abuse of a dominant position;
- The Database Directive[3], in particular its provisions governing the rights of lawful users of databases and exceptions to database rights;
- The Regulation on the free flow of non-personal data in the European Union, targeting non-personal data[4];
- The eCommerce Directive: containing rules for information society services, in particular the liability for intermediary service providers (caching, hosting and mere conduit)[5];
- The Copyright DSM Directive, and in particular its provisions in relation to text and data mining, both for the purposes of enabling scientific research and in general[6];
- The Trade Secrets Directive:[7] protects against unlawful acquisition, use and disclosure of trade secrets;
- The Software Directive: containing provisions on interoperability information[8];
- The Regulation on cross-border portability of online content services in the internal market (also known as the Portability Regulation)[9];
- Digital Content Directive: supply of digital content[10].

While it is not a regulatory instrument, the report below also examines the recent Recommendation of the European Commission on access to and preservation of scientific information[11], as a relevant policy document on this topic.

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT
[3] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN
[6] https://eur-lex.europa.eu/eli/dir/2019/790/oj
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024&from=EN
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R1128-20170630
[10] https://eur-lex.europa.eu/eli/dir/2019/770/oj
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0790&from=EN

2.3 Sector-specific rules

EU legislative initiatives applicable to data sharing within a particular sector or industry include notably:

- The Public Sector Information Directive (also known as the Open Data Directive): open data and the re-use of public sector information[12];
- The Market in Financial Instruments framework, comprising:
  - MIFID II (Directive), which targets trading data[13];
  - MIFIR (Regulation), which targets transaction reporting data;[14]
- The PSD2 Directive, aimed at financial transaction data[15] and at making this data available to certain new categories of service providers;
- The ePrivacy framework aiming (among other goals) to safeguard the security and confidentiality of electronic communications:
  - currently consisting of the ePrivacy Directive of 2002[16] and the consolidated Directive of 2009[17] (the latter often being referred to as the Cookies Directive), targeting direct marketing data and data collected by means of cookies;
  - in the future, this Directive may be replaced by the proposal for an ePrivacy Regulation: electronic communications data of individuals and companies[18];
- Commission delegated Regulation No 886/2013 on road safety-related minimum universal traffic data[19];
- The European Electronic Communications Code: electronic communication data[20];
- The Electricity Directive 2009/72/EC[21] and the recast Electricity Directive 2019/944: energy data[22];
- The RMI Framework, comprising:
  - Regulation (EC) No 715/2007: vehicle repair and maintenance data for light-duty vehicles[23];

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=EN
[18] https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0886&from=EN
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG
[21] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32009L0072
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944
[23] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0715&from=EN

- Regulation (EC) No 595/2009: vehicle repair and maintenance data for heavy-duty vehicles[24];

- The REACH Regulation in relation to chemical safety data[25];
- The Medicines Approval Regulation in relation to pharmaceutical testing data (human and veterinary use)[26];
- The Energy Efficiency Directive 2018[27], which targets smart meter data;
- The Gas Directives and its provisions on energy consumption data[28];
- The Clinical Trial Regulation: clinical trial data[29];
- The Code of Conduct on agricultural data sharing: agricultural data[30];
- INSPIRE Directive 2012[31] and consolidated Directive 2019: geographical data; [32]
- Radio spectrum Decision: freedom to receive and disseminate information and ideas.[33]
- The rules applicable to EU research and innovation framework programmes.

As indicated in the introduction, this overview will be maintained and expanded throughout the project.

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0595&from=EN
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1907&from=EN
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0726&from=EN
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L2002&from=EN
[28] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32009L0073
[29] https://ec.europa.eu/health//sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf
[30] https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf; https://www.ecpa.eu/news/code-conduct-agricultural-data-sharing-signing
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0002&from=EN
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02007L0002-20190626&from=EN
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0676&from=EN

3 Analysis of the EU acquis applicable to data sharing

A summary explanation is provided below of each relevant EU instrument that touches upon data sharing, using the general approach explained above. General trends and conclusions are provided in the subsequent sections.

3.1 General and horizontal legislation

3.1.1 The General Data Protection Regulation (GDPR)

3.1.1.1 Short summary

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**GDPR**) sets outs rules in relation to the processing of personal data in the EU and of EU residents. This Regulation became applicable on 25 May 2018.

The concept of personal data is defined broadly as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4 (1)). Without going into too much detail, the GDPR defines a series of principles and requirements that must be adhered to when processing personal data within the scope of the GDPR.

The notion of data processing is similarly broad, and includes "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4 (2)). Data sharing would therefore clearly constitute a data processing activity as defined under the GDPR – provided of course that the data being shared constitutes or contains personal data as described above. Given the breadth of the concept of personal data, it is clear that much data sharing will fall within the scope of the GDPR.

One of the central innovations of the GDPR – compared to the preceding legal framework, the Data Protection Directive 95/46/EC – is the introduction of the accountability principle. This principle stresses that a data controller – i.e. the person defining the means and purposes of each act of personal data processing – must be able to demonstrate their compliance with the other principles of the GDPR. Rather than being a raising or a lowering of the bar of compliance, the accountability principle provides a different way of looking at data protection compliance: while innovative data

processing activities remain possible, it is the duty of a data controller to continuously assess and be able to justify the compliance of their activities with the law.

It is worth underlining that data sharing under the GDPR can take many different forms, corresponding to diverging legal relationships with differing requirements.

- one might consider the simple case of a data controller making personal data available to the person it relates to (the data subject); this is a fairly simple interacting in which the direct involvement of both the controller and the data subject provides an initial safeguard against abuses;
- a separate case is that in which a controller 'shares' data with its service provider, who is bound to the controller by a written agreement. The GDPR would construe such a case as a data controller entrusting certain contractually defined processing activities to a data processor; provided that the processor is selected carefully and that an appropriate written agreement has been implement (as required under Article 28 of the GDPR), this situation too need not present significant data protection risks.
- there is also the case where one data controller makes data available to another data controller, where that second data controller will use the data for entirely separate purposes and using separate means than the first one. This type of interaction presents a series of unique challenges, notably in ensuring that there is a clear legal basis for the transfer and for the further processing, and that the further processing is compatible with the initial purposes of processing.
- finally, more complex cases can occur where multiple legal entities are jointly responsible for a common (shared) data processing activity; this case is described as joint controllership under Article 26 of the GDPR, and requires the joint controllers to implement appropriate arrangements - habitually but not necessarily taking the form of contracts – in order to ensure that the GDPR is complied with.

As was already indicated above, personal data sharing – and thus most of the GDPR – is out of scope of this report, which focuses on EU law applicable to sharing of *non-personal data*. For that reason, the GDPR is not examined in this report at a great level of detail. None the less, the GDPR still has a strong shaping influence on data sharing practices in the EU, simply due to the breadth of the personal data concept and because of the prevalence of mixed data sets comprising both personal and non-personal data. Moreover, as we shall show below the GDPR also implies the need to share non-personal data in some circumstances. These will be the focus of the comments below.

3.1.1.2 Objectives in relation to data sharing

Given that one of its objectives is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, it is not surprising that the GDPR has no explicit objectives in relation to data sharing. Rather, the sharing of personal data tends to be possible only under specific constraints, i.e. by ensuring that the principles of the GDPR can be adhered to. These include e.g. the proportionality and purpose limitation principles, implying that data can only be shared when and insofar as this is necessary to achieve the legitimate purposes of the data controller(s), and that shared data may only be used for the purposes communicated to the data subjects.

None the less, there are certain forms of data sharing which are supported or required under the GDPR, which relate notably to non-personal data. Key examples include:

- the transparency obligations towards data subjects (Article 13-14), comprising the obligation to inform them about crucial aspects of the data processing activities. In practical terms, this is a duty to share information about some business practices within the data controller;
- interactions between controllers and processors, or between data controllers, requiring them to exchange information on their data processing practices, at least to the extent that this is necessary to implement appropriate contractual safeguards (Article 28). An example is the identification of security measures that each party will implement; a baseline of information on security practices therefore needs to be shared between the parties.
- incident information. Notably, the GDPR requires breach notifications (including a description of incidents, anticipated impacts and mitigation measures) to be communicated to data protection authorities (with certain exceptions) and (in some cases) to the affected data subjects (Articles 32 and 33). Furthermore, data processors are required to submit such notifications to their data controllers. This is a form of obligatory data sharing which increases transparency and security awareness, and which improves security risk management.
- in a comparable vein, data protection impact assessments must be conducted in case of innovative or high-risk data processing activities. If the assessment reveals a residual risk that may not be appropriately mitigated, the data controller must engage in a prior consultation with the data protection authority; again, this is a form of obligatory data sharing (Article 37-38).
- supervision by data protection authorities (Article 31), which have the right to inspect data processing practices towards controllers and processors in their jurisdiction, including the right to request documentary evidence relating to data processing activities. Again, this is a form of mandatory data sharing (generally demand driven, i.e. in response to a request from a data protection authority) as a way of improving compliance.

There are also provisions which more directly support data sharing, relating directly to personal data, notably the right to data portability. This is a right granted directly to a data subject (i.e. a natural person to whom personal data relates), and which is therefore not available to legal entities. It allows the data subject under certain conditions "*to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided*". Since this aspect relates directly to personal data and is therefore out of scope of this report, it will not be examined in detail here.

3.1.1.3 Parties targeted or affected

The GDPR applies to data controllers, data processors and data subjects as described above. It is worth noting that, under Article 3, the GDPR's geographic reach is extraterritorial: it *"applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

(a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

(b) *the monitoring of their behaviour as far as their behaviour takes place within the Union".*

In other words, non-EU entities can potentially be bound by the GDPR.

3.1.1.4 Data targeted or affected

The GDPR formally applies to personal data only. Article 4.1 of the GDPR defines personal data as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

However, with respect to data sharing in particular, there are multiple examples where the GDPR requires non-personal data to be shared with third parties, as explained in section 3.1.2.2. above.

3.1.1.5 Short assessment of its impact

The principal impact of the GDPR relates to the sharing of personal data; a subject which is out of scope of the present report. None the less, the transparency and communication obligations that the GDPR creates go beyond the scope of personal data (although of course their applicability is always linked to the processing of personal data as a precondition to the applicability of the GDPR). This implies the need for data controllers and data processors to more systematically assess and document their data protection practices, and to describe these in a form that can be shared with other stakeholders as required by the GDPR. As such, while the GDPR itself is not conducive to encouraging data sharing (at least not in relation to personal data), it does establish an environment where data processing practices must be assessed in a manner that allows at least certain critical information to be shared.

3.1.2 Competition Law – TFEU

3.1.2.1 Short summary

At EU level, competition law is principally regulated by the Treaty on the Functioning of the European Union ("**TFEU**"). The relevant sections of the TFEU (notably the provisions of Article 101 and 102, which are the main provisions supporting European antitrust policy) aim to ensure that fair competition is not distorted in the internal market, and that the open market economy is protected. It fosters economic performance and offers consumers a wider selection of better-quality goods and services at more competitive prices and conditions. Article 101 of the TFEU contains a general prohibition against agreements between two or more independent market operators which restrict competition, including cartel agreements, and in particular those which:

"(a) directly or indirectly fix purchase or selling prices or any other trading conditions;

(b) limit or control production, markets, technical development, or investment;

(c) share markets or sources of supply;

(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".

Exemptions to this principle can be granted for (categories of) agreements, decisions or concerted practices which contribute "to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;

(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question".

Article 102 prohibits firms that hold a dominant position on a given market to abuse that position, specifically by:

"(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts" (Article 102, 2nd paragraph).

3.1.2.2 Objectives in relation to data sharing

There are several major reasons why competition law is worth calling out in particular in this report. Article 101 can of course apply in cases where data sharing in a specific instance is governed by agreements, decisions or concerted practices that violate the requirements of the TFEU by having as their object or effect the prevention, restriction or distortion of competition within the internal market. This could e.g. be the case where companies in the data economy share data on terms that exclude fair competition, are discriminatory, or make market entry for third parties prohibitively impractical. This implies that, when defining terms under which data is made available (e.g. licensing agreements), a company must assess whether it does not run afoul of the constraints imposed by Article 101.

In relation to Article 102, three other relevant factors of importance can be underlined. The first is its potential application to data sharing practices. Article 102 of course does not call out data sharing in particular, but is drafted to generally prevent companies that have a dominant market position from abusing that position to the detriment of consumers.

There are several instances where abuses can occur in relation to data sharing. One could consider the situation where a company would like to access and use particular data held by another company. That data holding company may be a direct competitor who holds commercially relevant information – e.g. a database with information on a specific market, such as available real estate in a specific geography – or it may be a company with ancillary business activities, such as a cloud provider whose

platform could be expanded with new functionalities if it would be willing to allow third parties to create them and access the data it holds.

Normally, the two companies would enter into negotiations to conclude an agreement establishing mutually agreeable data sharing modalities. However, if the company holding the information does not see sufficient economic interest in granting the other company access to the information, it will most likely be reluctant to share the information at all, or subject the availability or use of the data to terms which are manifestly unacceptable. This becomes problematic if the company holding the information enjoys dominant position within the common market or in a substantial part of it, as described in Article 102, and abuses its position to refuse the other company access to that market. A basic example could be if the dominant company only allows data sharing under unequal or discriminatory terms, or if it abuses its dominant position to ensure its control over potential competitors.

In that case, the provisions of the TFEU could be used to address the abuse, e.g. by requiring data sharing practices which are more conducive to competition.

A prominent (and early) example of this approach is the *Magill case* of 1995, in which the CJEU held that broadcasting companies in Ireland which enjoyed a de facto monopoly over the information used to compile listings for the television programmes received in most households in Ireland and in Northern Ireland, were obliged to supply information about weekly programmes to the publishing company Magill TV Guide Ltd. The latter had wanted to introduce a comprehensive television guide, and the information requested from the broadcasting companies was the raw source material required to establish such a guide. Without the cooperation of the broadcasting companies, it would be locked out of the market and unable to compete under reasonable terms.

The CJEU ruled that: *"[t]he appellants' refusal to provide basic information by relying on national copyright provisions thus prevented the appearance of a new product, a comprehensive weekly guide to television programmes, which the appellants did not offer and for which there was a potential consumer demand. Such refusal constitutes an abuse under heading (b) of the second paragraph of Article 86 of the Treaty [now Article 102 (b) §2 TFEU]" and: "[…] the appellants, by their conduct, reserved to themselves the secondary market of weekly television guides by excluding all competition on that market (see the judgment in Joined Cases 6/73 and 7/73 Commercial Solvents v Commission [1974] ECR 223, paragraph 25) since they denied access to the basic information which is the raw material indispensable for the compilation of such a guide."* The broadcasting companies' argumentation that this information was protected by copyright, was considered by the Court to be insufficient to justify the constraints on its accessibility and was refused.[34] A similar conclusion was drawn by the Court of First Instance (predecessor of the General Court) in the *Microsoft case*[35].

It appears from this case law that competition law is a viable a legal instrument to force companies holding a dominant position to share information with others if they abuse their position to deny other companies' entrance to the internal market, even when there are no comparable products or services in the relevant market yet. The ruling is particularly noteworthy because the broadcasting companies were not offering a broadcasting guide with which Magill would be competing, nor were

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61991CJ0241, especially §54-§56.

[35] Case T-201/04, CFI 28 April 2005, Microsoft Corp. and others v Commission of the European Communities and others: http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dbdbf931114dab46eb9c81a50729a1d8ad.e34KaxiLc3qMb40Rch0SaxuLc390?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=55664&occ=first&dir=&cid=432394

they sharing data with third parties that allowed those parties (but not Magill) to create such a guide. The broadcasting companies simply acted in a manner that made it impossible for such a product or service to be provided by denying access to data, even though there would conceivably be a market for it. In other words, a data sharing claim based on EU antitrust rules against a dominant party is conceptually viable even when that party is not using the data itself or making it available to other parties to provide a comparable product or service. The act of making innovation impossible by refusing to make data available to third parties can as such already be grounds for intervention, at least in some instances.

The second reason why Article 102 is particularly salient to data sharing is the importance accorded to competition law in the digital era, notably against the backdrop of platforms, digital ecosystems, and the data economy, where a small number of incumbent market players can capture large segments of a market, making it significantly harder for new entrants to compete or innovate.

It is worth calling out in particular the findings from the report "Competition policy for the digital era" procured in 2019 by the European Commission – Directorate-General for Competition.[36] The report stressed, among other matters, the importance of assessing strategies employed by dominant platforms aimed at reducing the competitive pressure they face. It recommended that such strategies should be forbidden in the absence of clearly documented consumer welfare gains. On this point, the report called for less emphasis on analysis of market definition – also because a platform itself could in practice be considered a relevant market - and more emphasis on theories of harm and identification of anti-competitive strategies. When it comes to dominant platforms, the report argued that they should act as de facto regulators themselves by establishing rules and policies that would be conducive to competition unless there would be an objective justification to adopt more restrictive approaches. A proactive data interoperability policy – i.e. ensuring that data can be ported more easily from one service to another - can be a remedy against anti-competitive leveraging of market power into markets for complementary services. Where vertical and conglomerate integration and the rise of powerful ecosystems may raise concerns, requiring dominant players to ensure data interoperability may be an attractive and efficient alternative to calling for the break-up of firms – a way that allows us to continue to benefit from the efficiencies of integration.

The third reason behind the interest in Article 102 is the increased focus from competition authorities on data sharing. This can be witnessed in a recent ruling of German competition authority, the Bundeskartellamt, regarding the interplay between data protection and competition law, against Facebook[37]. Although sharing of personal data falls outside the scope of this report, it is none the less relevant due to its potential impact on data sharing practices in the EU. It should be noted though that this decision is not yet final since Facebook appealed to the Düsseldorf Higher Regional Court. In its ruling, the German competition authority prohibited Facebook from combining data of users across its own suite of social platforms without their consent. Facebook, as a company with a dominant position in the German market, is subject to stringent obligations under competition law

[36] https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

[37] The reason why the Bundeskartellamt did not focus on the Article 102 TFEU is that so far, however, only the case-law of the highest German court has been established which can take into account constitutional or other legal principles (in this case data protection) in assessing abusive practices of a dominant company, see page 6: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6 and https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

(cumulatively of course with its data protection obligations). The Bundeskartellamt held that when access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is not only relevant for data protection authorities, but also becomes relevant for competition authorities. On that basis, the Bundeskartellamt concluded that the extent to which Facebook collects, merges and uses data in user accounts constitutes an abuse of a dominant position and that Facebook's conduct represents an exploitative abuse. Important to note however is that the Bundeskartellamt based its assessment on German competition law, although, according to the Bundeskartellamt, Article 102 TFEU could also apply in this context. Although it is not necessarily a new approach for a competition authority to take decisive factors, such as data, into account when assessing the abuse of a dominant position of a company, it is striking that the way data is being collected is of such paramount importance in the context of a competition issue and that even the compliance with data protection legislation is considered in the assessment.

3.1.2.3 Parties targeted or affected

Article 101 TFEU is relevant to any party that contributes to the establishment of agreements, decisions or concerted practices in relation to data sharing which may affect trade between Member States, and therefore to much of the data economy. While data sharing agreements and data licensing agreements can be pro-competition – and thus perfectly in line with the objectives of the internal market and the requirements of the TFEU – an assessment of potentially anticompetitive provisions is always required.

Article 102 TFEU – as well as national competition law – applies to companies with a dominant position in the market. The assessment of whether a company has a dominant position in a specific market is complex and is based on an interplay of many factors[38]. The first element consists of the definition of the relevant market, including the product market (i.e. identifying which products and/or services would be considered substitutes to the examined product/service by consumers) and the geographic market (where conditions of competition are homogeneous), and the second step being to assess dominance. Market share is a key factor here, but other elements are relevant too. These include ease of market entry, buying power and general economic size/strength/market power, and presence in a full product/service chain (vertical integration).

The Magill case already considered exclusive data holdership to be relevant, and the aforementioned Report on Competition policy for the digital era identified the following additional relevant factors for data sharing/data pooling agreements:

"• What "type" of data is shared or pooled: contextual, e.g. maps, and aggregated data, e.g. frequency tables for accidents, or individual-level data?

• Are individual-level or machine data being pooled together but used anonymously, or is the data personally identifiable?

• Are technical measures put in place to limit and/or control how the data is being used?" Inversely, the presence of technical measures to facilitate data sharing and reuse (such as data interoperability and API services) could be a relevant counter-indicator.

[38] See https://ec.europa.eu/competition/antitrust/procedures_102_en.html

Other affected parties are of course the intended beneficiaries, including competitors, aspiring innovators (as in Magill), and ultimately any natural and legal persons who rely on the benefits of the internal market. Any citizen or business which suffers harm as a result of a breach of the EU competition rules is entitled to claim compensation from the party who caused it.

3.1.2.4 Data targeted or affected

As appears from the case law, Articles 101 and 102 can apply to any type of data to the extent that the practices surrounding the accessibility or usage of the data are found to be abusive under the TFEU.

3.1.2.5 Short assessment of its impact

Antitrust law can be a powerful instrument in combating anti-competitive practices in relation to data sharing. In case of established infringements, Council Regulation 1/2003[39], based on Article 103 TFEU, allows the Commission to impose fines based on the gravity and the duration of the infringement, capped at a maximum of 10% of an infringing company's turnover. Thus, the financial penalties alone are a strong incentive towards competitive practices.

Both the *Magill case* and the *German Facebook case* show – though in another way - the impact of competition law, and more particularly the abuse of a dominant position on the processing of personal and non-personal data.

It appears from the ruling of the CJEU in the *Magill case* and other cases that in the event of an abuse of a dominant position, competition law may be used as a tool to ensure data sharing for the sake of the effective functioning of the internal market. Competition law can potentially be used to force companies with a dominant position to share certain information to prevent that such companies preclude others from entering the internal market.

None the less, this does not imply that any aspiring innovator or competitor can simply claim access to data, even from a dominant party. The aforementioned report on "Competition policy for the digital era" advised caution, noting that thorough analysis would be required as to whether such access is truly indispensable, taking into account different forms of data, levels of data access, and data uses. A direct application of prevailing essential facilities doctrine (which favours the granting of accessibility of infrastructure only when this is essential to bring a product or service to the market[40]) would not easily apply to data without negative impacts on innovation and competition. When data access is not indispensable to compete, public authorities should refrain from intervention, according to the authors.

Furthermore, the relevance of the interplay between competition law and data protection law has become clear in the *German Facebook case*. It appears from the ruling of the German competition authority that to the extent that data are a decisive factor for establishing a company's dominant position, the compliance with data protection legislation, i.e. the way data is used, is considered in the assessment of abuse of a dominant position.

---

[39] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty; see https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003R0001

[40] Or more formally, the test implies that a company with a dominant position in the provision of a facility, product or service which is indispensable to compete in a downstream market abuses its dominant position where, without objective justification, it refuses to grant access to this facility, product or service, with the effect that all effective competition in a downstream market is eliminated; Case C-7/97, Bronner, EU:C:1998:569; Case T-167/08, Microsoft v Commission, EU:T:2012:323

3.1.3 The Database Directive

3.1.3.1 Short summary

The Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (**Database Directive**) establishes a legal framework for two types of intellectual property rights relating to databases. Firstly, it clarifies that databases can qualify for copyright protection if they satisfy the creativity criterion that applies to any other copyright protected work, i.e. if the databases "by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation" (Article 3.1 of the Directive). Secondly, it creates an entirely new type of intellectual property right, a so called *sui generis* right, which applies to any database "which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database" (Article 7.1). As a side note, the Open Data Directive states that this right shall not be exercised by public sector bodies in order to prevent the re-use of documents or to restrict re-use beyond the limits set by the Open Data Directive (Article 1.6 Open Data Directive).

In other words, following its implementation into national law, databases in the EU can be subject to copyright protection by virtue of the creativity criterion, and/or to *sui generis* protection by virtue of the investment involved. The regimes can apply cumulatively – a single database may therefore be covered by both rights – and the protection of the database as a whole is unrelated to any protections of individual works included in a database – e.g. a database of photos may fall under copyright and *sui generis* rights, while the individual photos each are covered by copyright.

If *sui generis* rights are granted, the Directive defines harmonised rights and obligations of lawful users, notably the right to extract and/or re-utilize insubstantial parts of its contents, in combination with provisions aiming to safeguard the normal exploitation of the database and the legitimate interests of the maker of the database (article 8), as will be explained further below. Furthermore, the Directive foresees specific exceptions, allowing lawful users of a database which is made available to the public to extract or re-utilize a substantial part of its contents:

- *"in the case of extraction for private purposes of the contents of a non-electronic database;*
- *in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;*
- *in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure"*. (Article 9)

The Directive is notable because it creates both a new legal protection regime for databases that goes beyond what traditional copyright might allow, and because of the ample exception regime that allows for even 'substantial' extraction or re-utilisation of the database contents.

As will be explained further below, additional exceptions to the Database Directive have been established through the Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790). While this more recent Directive did not directly amend the Database Directive at the EU level, it does oblige Member States to implement additional exceptions into their national laws which

implemented the Database Directive. Notably, it requires Member States to foresee new exceptions, both in relation to copyright and *sui generis* rights, relating to:

- Text and data mining for the purposes of scientific research
- Exception or limitation for text and data mining
- Use of works and other subject matter in digital and cross-border teaching activities
- Preservation of cultural heritage
- Use of out-of-commerce works and other subject matter by cultural heritage institutions

The scope and impact of these exceptions will be discussed in the section of this report on the Directive on Copyright in the Digital Single Market.

3.1.3.2 Objectives in relation to data sharing

The general objective of the legislator was to provide an additional layer of legal protection for databases that was not available to database makers in most other areas of the world, based on the conviction that this would provide a stimulus for the database creation industry. As the recitals to the Directive note, "*Whereas there is at present a very great imbalance in the level of investment in the database sector both as between the Member States and between the Community and the world's largest database-producing third countries; Whereas such an investment in modern information storage and processing systems will not take place within the Community unless a stable and uniform legal protection regime is introduced for the protection of the rights of makers of databases*". Given these drivers, sharing of data was not high on the list of priorities.

None the less, the legislator was also conscious of the risk of undesired side effects by creating legislation that would stifle innovation beyond what was necessary. For that reason, the Directive clearly established certain rights and obligations of lawful users of a database in Article 8. As a central right, the Directive notes that the maker of a database which is made available to the public may not prevent a lawful user from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Thus, in relation to 'insubstantial' parts of a database, the Directive actively facilitates data sharing (as a form of use) for lawful users.

This general right is combined with obligations for lawful users that protect the interests of the database maker. A lawful user of a database which is made available to the public may not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database (Article 8.2). Furthermore, a lawful user of a database which is made available to the public may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the database (Article 8.3). Thus, the fact that a database is made available to the public does not entail that any use is permissible; the database maker's interests and exploitation rights must always be taken under consideration.

In addition, carve-outs were simultaneously enabled – but not made mandatory – in Article 9, that allow Member States to permit extraction for private use, teaching or scientific research purposes, and extraction and re-use for purposes of public security or an administrative or judicial procedure. In those cases, lawful users of databases which are made available to the public enjoy ample – indeed, nearly unlimited – extraction and/or reutilisation rights.

3.1.3.3 Parties targeted or affected

There are generally three categories of parties affected:

- the author of a database, in case of copyright protected databases. This is defined as "the natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the rightholder by that legislation";
- the maker of a database, in case of *sui generis* protected databases, described in the recitals to the Directive as "the person who takes the initiative and the risk of investing", clarifying that (contrary to copyright law) this excludes subcontractors in particular from the definition of a maker and;
- the lawful users of a publicly available database who enjoy the rights and exceptions defined in the Directive, subject to the obligations also defined therein.

3.1.3.4 Data targeted or affected

The Directive applies to databases in general, defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Article 1.2). Any data in such a database, provided that the database is subject to copyright protection or *sui generis* protection, are affected by the provisions of the Directive in relation to extracting and re-utilization rights. The Directive itself expressly clarifies that software does not fall within its scope.

3.1.3.5 While the definition of a database is thus relatively broad and flexible, it is worth underlining that case law of the Court of Justice has somewhat eroded the potential scope of the Directive's provisions in relation to sui generis protection. Specifically, a series of 2004 decisions[41] indicated that the sui generis right does not apply to databases that are created as the by-products of the main activity of an organisation. As a result, many data sets which are automatically generated in the current data economy as the side effect of a principal service are out of scope, including any machine-generated data, IoT devices, data pools or data lakes used for big data analytics, etc; as well as databases that are created to facilitate a principal service such as e.g. patient records generated in the course of health care. Short assessment of its impact

Conceptually, the Database Directive could be expected to have a significant impact on the data economy and on data sharing, since it greatly expands the protections available for non-creative databases that none the less required a substantial investment. Extraction and/or re-use of substantial parts of the contents of a database protected by *sui generis* rights without the permission of the maker is only facilitated for (in the case of extraction) private use, teaching or scientific research, and (in the case of extraction and/or re-utilization) public security or an administrative or judicial procedure. As a result, the Directive might be expected to have a somewhat stifling effect. Inversely however, extraction and re-use of insubstantial parts of the contents are facilitated for any lawful users of publicly accessible databases.

[41] Mainly Fixtures Marketing Ltd v. Oy Veikkaus Ab (C-46/02, 9/11/2004), Fixtures Marketing Ltd v. Svenska Spel Ab (C-338/02, 9/11/2004) British Horseracing Board Ltd v. William Hill (C-203/02, 9/11/2004) Fixtures Marketing Ltd v. OPAP (C-444/02, 9/11/2004).

The case law referenced above partially undercuts that expected effect. Indeed the most recent 2018 evaluation of the Directive found that it was relevant and provided added value due to its ability to avoid fragmentation (i.e. the Directive stops Member State from diverging their laws on this point), but also noted that the sui generis right in particular "continues to have no proven impact on the overall production of databases in Europe, nor on the competitiveness of the EU database industry", and that "the application of the sui generis right in the data economy context should continue to be closely tracked".[42] Its impact is therefore likely relatively limited.

3.1.4 The Regulation on the free flow of non-personal data in the EU

3.1.4.1 Short summary

Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (**Free Flow Regulation**) became applicable as of 28 May 2019. It is a recent regulatory initiative that aims to remove some barriers to the free flow of non-personal data in the internal market.

More specifically, it aims to ensure that every organisation can store or otherwise process data anywhere in the European Union, while ensuring that national supervisors retain appropriate regulatory controls. Member States are therefore required to review their legislation to ensure that they do not retain laws which are contrary to this principle. Some exceptions are provided, notably where legislative data localisation requirements can be justified by the Member State on grounds of public security in compliance with the principle of proportionality.

In the past, the free flow of data (personal and non-personal) has been hindered by the presence of so-called "data localisation requirements". A data localisation requirement is a restriction on the flow of data from one country to another. This requirement raises the cost of conducting business across borders. In the EU, more than 60 restrictions were identified in 25 jurisdictions.[43]

Especially cloud service providers are affected by data localisation requirements. According to them, these restrictions undermine the cloud business model, since these restrictions prevent cloud service providers from accessing markets where they do not have their own data centre and they prevent end-users from using cloud services provided from another EU Member State than their Member State of residence.[44] The Free Flow Regulation acknowledges that our economy relies more and more on data and recognises electronic data as the centre of innovative systems and societies. Together with the GDPR, it creates a common European space for data by both allowing the free movement of personal data within the EU.

In relation to data sharing, the Regulation is notably relevant due to its provisions on data porting, as will be explained below.

[42] See https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51764

[43] See Annex 5 to the Commission staff working document impact assessment, citing: LE Europe study (SMART 2015/0016, pg. 37) and Timelex' study "SMART 0054/2016", Commission, 'Impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' Staff Working Document) SWD 2017, 304 final

[44] European Commission, "Annex to the Synopsis Report. Detailed Analysis of the Public Online Consultation Results on 'Building a European Data Economy", 2017 and Bird & Bird, "Data-related legal, ethical and social issues", pg 42, 2019, available at: https://www.twobirds.com/en/news/articles/2019/global/eu-data-economy-legal-ethical-and-social-issues.

3.1.4.2 Objectives in relation to data sharing

While much of the Regulation focuses on eliminating data localisation restrictions wherever possible and on enabling regulatory controls, from a data sharing perspective its provisions on data porting (notably Article 6) are particularly relevant.

In a nutshell, Article 6 requires the Commission to "encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data".

In other words, the data porting principle in the Regulation encourages stakeholders to voluntarily provide services that facilitate the movement of data from one service provider to another, or to simply port data back to its own IT systems. Information on these services should be provided to aspiring customers prior to contract conclusion.

In terms of timing, the development of such codes of conduct should be completed by 29 November 2019, and effective implementation should follow by 29 May 2020.

3.1.4.3 Parties targeted or affected

If codes of conduct are effectively implemented, the Regulation would ensure that data sharing is facilitated from any provider of data processing services to users residing or having an establishment in the Union, including those who provide data processing services in the Union without an establishment in the Union.

The 'data sharing' aspect allows notably professional users (defined as any person including a public authority or a body governed by public law, using or requesting a data processing service for purposes related to its trade, business, craft, profession or task) of such services to request their data back, or to move it to competing service providers. While the sharing of data is limited to these parties – providers of data processing services and their professional users - porting is thus turned into an instrument that facilitates data flows and avoids lock-in effects.

3.1.4.4 Data targeted or affected

The Regulation states that it "applies to the processing of electronic data other than personal data in the EU, which is:

- provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the EU; or
- carried out by a natural or legal person residing or having an establishment in the EU for its own needs".

Examples of such data are data sets created or used in the context of the Internet of Things, artificial intelligence and machine learning, for instance as used in automated industrial production processes.

As the name of the Regulation already stresses, it emphatically focuses on non-personal data – indeed, its formal definition of data in Article 3 (1) of the Regulation expressly excludes personal data. In practice, the line can be hard to draw, not only because of the broad scoping of the concept of

personal data, but also because a data set may comprise both personal and non-personal data. In such cases, the Regulation states that it applies only to the non-personal data part of the data set.

However, in some situations – e.g. in the case of data porting, where a customer wishes to obtain all of their data back - personal and non-personal data in a data set can be inextricably linked, and it may not even be possible for a service provider to limit its application of the Regulation to only personal data. It will be complex to determine which Regulation applies to which part of the dataset. The possible extent of the term "personal data" was clarified by the CJEU in the *Breyer case*[45], which concerned IP addresses. The CJEU clarified that a piece of information can be considered personal data whenever additional information can be sought from third parties to identify a data subject. When applying the principles of *Breyer* in practice, means that data items which in the first place seem to constitute non-personal data, may probably fall under the scope of the GDPR's definition of personal data. This leads to uncertainty as to what information will fall within the scope of the Free Flow Regulation.

To assist in addressing ambiguities, guidance has been provided by the European Commission on the interaction between the free flow of non-personal data regulation and the GDPR, and the application of the Free Flow Regulation on mixed data sets[46].

3.1.4.5 Short assessment of its impact

The Free Flow Regulation abolishes data localisation requirements in the EU and hence, permits businesses and public sector bodies to choose cheaper and more innovative services and allows cloud service providers to expand their businesses throughout Europe.

More specifically, for professional users the provisions on data porting – assuming that appropriate codes of conduct are implemented – facilitate data sharing from one service provider to another. From a broader perspective, the mere ability to automatically retrieve one's own data is conducive to establishing an economic, technical and business environment where data sharing is more keenly encouraged and adopted – once it is practically feasibly to obtain a data set "in a structured, commonly used and machine-readable format", it becomes markedly easier to exchange this data set with other parties, also in use cases that formally fall outside the scope of the Regulation.

Of course, much depends on actual implementation of such codes of conduct. As a part of the execution of this goal, workstreams have been set up under the auspices of the European Commission in the form of several working groups on cloud computing switching/ data porting (SWIPO), which have produced draft codes of conduct covering both software as a service (SaaS) and infrastructure as a service (SaaS) cloud providers. These are currently not yet operational.

[45] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

[46] https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets

3.1.5 The eCommerce Directive

3.1.5.1 Short summary

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 **(eCommerce Directive)** regulates certain legal aspects of information society services (i.e. any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services; the term is broadly equivalent to an online service) within the European Union. It aims at promoting electronic commerce and at ensuring net neutrality, by removing obstacles to cross-border online services in the EU and provide legal certainty to business and citizens.

In transposing the eCommerce Directive, Member States should adopt national measures ensuring the free movement of information society services, in particular ensuring that such services are not subject to any prior authorization regimes. Member States should approximate their national laws with regard to: (a) the establishment of service providers; (b) commercial communications; (c) electronic contracts; (d) the liability of intermediaries; (e) codes of conduct; (f) out-of-court dispute settlement; (g) court actions and (h) cooperation between Member States.

3.1.5.2 Objectives in relation to data sharing

In terms of data sharing in the context of the eCommerce Directive, one of its recitals confirms that the legislative data protection framework (such as the GDPR and Directive on privacy and electronic communications) is fully applicable to information society services. Hence, the eCommerce Directive does not impose any additional explicit obligations as regards the sharing of personal data between online service providers in different Member States, nor does it contain any explicit objectives on this point.

However, the Directive is none the less relevant to data sharing as a whole, due to the fact that it also contains rules relating to liability for three types of intermediary online services, namely “mere conduit”, “caching” and “hosting”, as described in Section 4 of the Directive (Articles 12-14), “Liability of intermediary service providers”. Since these services are common tools for enabling data sharing, the Directive has broader relevance.

Without going into too much detail:

- mere conduit is described in the Directive as “the transmission in a communication network of information provided by a recipient of the service, for the provision of access to a communication network”;
- caching is described as “the transmission in a communication network of information provided by a recipient of the service performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request” and;
- hosting is described as “the storage of information provided by a recipient of the service”.

In these cases, such service providers are not liable for the use of their services provided that they do not curate the data passing through their services, that they have no actual knowledge of unlawful use of their services, and that they act expeditiously when they received notifications of unlawful use. The reasoning behind this is to protect intermediaries who are not actively involved in the

creation, identification, promotion of the harmful activity but who are only involved in the passive transit or hosting of the infringing content. Accordingly, the Directive clarifies in its Article 15 that Member States cannot make these service providers subject to general obligations to monitor the use of their services, but eventually only to inform competent public authorities of illegal activities they happen to have knowledge for and of information enabling the identification of recipients of their services with whom they have storage agreements).

It is worth noting though that the emergence of new technologies and the complexity of the data value chain put pressure on the current safe harbour regime, which, at the time, did not take into account new services such as AI, IoT and big data.

The Directive also contains general transparency obligations (notably under Article 10), but since these are relatively high level and generally do not pertain to business-critical information, it would be disproportionate to construe those as a form of data sharing.

3.1.5.3 Parties targeted or affected

The Parties targeted or affected by the eCommerce Directive are principally the providers of information society services and their customers. In particular, the eCommerce Directive is important to intermediaries with regard to the safe harbor regime as described above.

3.1.5.4 Data targeted or affected

In the context of the eCommerce Directive, many different types of information can be involved; the Directive has no inherent limitations or constraints. By ways of examples:

- To allow interconnections between private communications networks, service providers act as mere conduits in sharing data messages (voice, text, video, order forms, etc.) between each other.
- To expedite data transfer speeds and reliability, data from a video streaming service is stored temporarily in geographically dispersed servers that can respond quickly to local needs. This qualifies as a caching service.
- A company wishes to obtain open source software. It uses an online repository, which qualifies as a hosting service.

As these examples show, potentially any type of data can fall within the scope of the Directive.

3.1.5.5 Short assessment of its impact

The eCommerce Directive was one of the very first EU initiatives to reduce online barriers between Member States. Since then, there has been a wide range of other EU initiatives to further reduce these barriers. The way in which the Internet was used by consumers in 2000 is very different from the way in which consumers today use the Internet to shop online. The EU's 2015 Digital Single Market Strategy aimed to address this challenge by taking new and more targeted measures, including:

- PSD2;
- new rules on cross-border parcel delivery services;
- new rules on geoblocking;
- revised consumer protection rules that enter into force in 2020;

- new VAT rules for online sales of goods and services that will enter into force in 2021.

None the less, the eCommerce Directive remains important in terms of defining the principles behind the liability of intermediaries. The approach is however increasingly put under pressure by new technologies, and notable case law exists on this topic. A prominent example is the legal proceeding between cosmetic manufacturer L'Oréal and the online marketplace eBay.[47] Relevant for this report was the question whether eBay, as a hosting provider, could be held liable for a trademark infringement committed by merchants operating through its website. The CJEU ruled in 2011 that the liability exemption of Article 14.1 of the Directive only applies when the information society service merely acts as an intermediary and not when it "*plays an active role of such a kind as to give it knowledge of, or control over, those data [entered by recipients].*" The Court in the present case found that eBay generally processes data entered by its customer-sellers; however, in some cases, it provides assistance to optimize or promote certain offers for sale. Therefore, it cannot not rely on the exemption from liability offered in Article 14.1 of the Directive, since its role is not purely passive.

Additionally, the court noted that, where the operator of the online marketplace does not play an active role in processing data and optimizing the presentation of the offers for sale, it cannot escape liability for damages *"if it was aware of the facts or circumstances on the basis of which a diligent economic operator should have realized that the offers for sale in question were unlawful."*

A year earlier, the Court had applied a similar, but less explicit, reasoning in the *Google v Louis Vuitton and others case*[48], which related however to registered trademarks being available for purchase as search keywords to competitors in search engines (i.e. the fact that a competitor could purchase advertisements on another company's trademarked name in the Google search engine, so that the competitor's products and services would be shown when anyone would search for the original company's trademarked name). The Court ruled that the storage and display of such a trademark by a search engine (as a part of the advertising search practice) did not constitute a use of that trademark within the meaning of EU trademark law, and more relevantly to this case, that the eCommerce Directive's Article 14 in relation to hosting services should apply to search engine providers as well, at least "in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned".

Accordingly, when the provision of the service of an information society service goes beyond the technical and automatic processing of data, or if the information society service has actual knowledge of an unlawful activity or information, it cannot benefit from the liability exemption. If information society providers are unable to take advantage of this exception, they will be obliged to monitor the data they process more closely, otherwise they may be held liable.

It is worth underlining that due to the pressure put on the current safe harbor regime – especially since the emergence of new technologies, the complexity of data and the more active role of

[47] http://curia.europa.eu/juris/liste.jsf?num=C-324/09.
[48] http://curia.europa.eu/juris/liste.jsf?num=C-236/08

intermediaries – the EU Commission examined the rules related to such intermediaries, as part of its Digital Single Market Strategy. The next Chapter describes these new rules in more detail.

3.1.6 Copyright DSM Directive

3.1.6.1 Short summary

The Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC ("**Copyright DSM Directive**") aims to modernise copyright law for the digital environment. Copyright protects various types of works, as long as they are original and can be expressed in a material, concrete form. In the context of data sharing, this means that copyright protection can be granted to data representing a creative expression, but not to non-creative factual data as such.

For the purposes of this report, the Directive is principally relevant in regard to the newly created copyright exceptions for text and data mining, and the rules on so-called online content-sharing service providers. Besides this, the Directive also includes provisions aiming to protect press publications and provides a more comprehensive framework for collective licensing practices and out of commerce works. These will however not be elaborated on below.

3.1.6.2 Objectives in relation to data sharing

The older Directive on the harmonisation of certain aspects of copyright and related rights in the information society (i.e. the so-called Information Society Directive)[49] already harmonised and modernised the European legal framework in relation to copyrights and related rights, and brought it in line with the emergence of the Internet and the digital economy. However, several more current key economic trends created a need for a new revision, which was the object of the Copyright DSM Directive.

Particularly relevant for this report is the legal framework set out by the Copyright DSM Directive in relation to text and data mining, and for so-called Online Content-Sharing Service Providers ("OCSSPs").

Text and data mining are broadly defined in the Directive as "any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations". This functional description aims to encompass a broad range of existing and future analysis techniques.

Given that text and data mining can in certain instances involve acts in relation to works protected by copyright, by the sui generis database right or by both (such as the reproduction of works or other subject matter or the extraction of contents from a database), the Copyright DSM Directive provides for new exceptions to the exclusive right of reproduction and to the right to prevent extraction from a database for the purposes of text and data mining.

The Copyright DSM Directive distinguishes between text and data mining for the purposes of scientific research (Article 3) and text and data mining for other purposes (Article 4). Under Article 4 of the Directive Member States are obliged to implement exceptions to the copyright and database

[49] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

right for reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining, on the condition that this use for text and data mining purposes has not been expressly reserved by the rightholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online. In other words, the Directive appears to allow rightholders to unilaterally opt-out of this exception. From a data sharing/data access perspective, the principal beneficial impact is that this requires a conscious action ('expressly reserved') from the rightholder; i.e. the default status is that text and data mining are permitted if the rightholder takes no action.

Research organisations and cultural heritage institutions are granted a broader exception under Article 3, which requires Member States to implement exceptions to the copyright and database right for reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access, without any further conditions.

If data is copied for the purposes of enabling text and data mining (as would commonly be the case), copies must be stored with an appropriate level of security and may be retained for the purposes of scientific research, including for the verification of research results; and rightholders shall be allowed to apply measures to ensure the security and integrity of the networks and databases where the works or other subject matter are hosted. Thus, the data must remain appropriately protected against other (non-permitted) uses.

The newly introduced exceptions for text and data mining will likely have a positive effect on data access and data sharing, both for commercial enterprises in the data economy and research or cultural heritage institutions that envisage to engage in text and/or data mining for research purposes. Consequently, to the extent that not all rightholders will reserve their rights in regards text and data mining, it is expected that the new exceptions in the Copyright DSM Directive will significantly boost data access and sharing in the EU, and will drive innovation in the data economy as a whole.

As for Online Content-Sharing Service Providers, they are described in the Directive as "a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes" (article 2(6)). A non-exhaustive list of excluded categories of service providers is included as well[50].

The Directive requires such providers to obtain an authorisation from the rightholders in order to communicate or make available to the public works or other subject matter to the public uploaded by their users, which should also cover acts carried out by users of the services. The liability exemption in Article 14 of the eCommerce Directive is declared inapplicable to this specific type of service provider as far as copyright liability is concerned and under certain conditions. In particular, if no authorisations are obtained, service providers are liable for the behaviour of their users unless they can demonstrate that they have:

[50] Article 2(6) notes that "Providers of services, such as not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms, providers of electronic communications services as defined in Directive (EU) 2018/1972, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not 'online content-sharing service providers' within the meaning of this Directive". Note that this is a non-exhaustive list without defined common characteristics between the listed service providers that warrant their exclusion.

(a) made best efforts to obtain an authorisation, and

(b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event

(c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).

Providers of services of which have been available to the public for less than three years and which have an annual turnover below EUR 10 million are subject to lighter obligations. Larger service providers (with monthly unique visitors exceeding 5 million) conversely bear heavier obligations and must also "prevent further uploads of the notified works". Finally, service providers must "put in place an effective and expeditious complaint and redress mechanism" in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them.

3.1.6.3 Parties targeted or affected

While the parties targeted vary from provision to provision, the summary above would show that the principal targets are the online content-sharing service providers, who are targeted by new obligations and see some former protections from the eCommerce Directive removed.

The principal beneficiaries will be any parties seeking to lawfully access protected works for mining purposes, including actors in the data economy that rely on text and data mining for creating added value to their commercial or non-commercial activities. Their default position will be improved compared to the status quo. Other stakeholders such as research organisations and cultural heritage institutions will similarly benefit from the broader exceptions in regards text and data mining.

3.1.6.4 Data targeted or affected

Copyright protection can apply to every work, as long as it is original and expressed in a concrete form. In the context of big data analytics, only certain instances of analysis through text and data mining will relate to copyright protected works (such as photographs, scientific articles, newspaper publications etc.). Mining other data that is not part of a copyright protected work will not result in a copyright restricted reproduction and will thus not have to rely on the exception on the exclusive rights of the author (or rightholders) for text and data mining purposes.

This does not mean, however, that individual dataset which are not creative and are therefore not subject to copyrights cannot gain originality once they relate to other information or once they are presented in an original way.[51]But it should be emphasized that non-original sets of data or non-original combinations of such data are not copyright protected and can be mined without relying on the exceptions for text and data mining. More so, copyright protection does not extend to the data incorporated in original works. Only when (sets of) copyright protected works are mined, reproductions may run counter to the rights of the author (or rightholders) and text and data mining will be conditional upon the fulfilling of the provision of Article 3 and 4 of the Copyright DSM Directive.

[51] See Bird & Bird, "Data-related legal, ethical and social issues", pg 54, 2019.

3.1.6.5 Short assessment of its impact

As mentioned above, the exceptions relating to text and data mining that are introduced by Article 3 and 4 of the Copyright DSM Directive will most likely have a positive, enhancing effect to the data economy and can increase innovation in the field of data access and sharing. Nevertheless, it should be acknowledged that innovators can still be curbed by rightholders, who can still reserve their rights as regards text and data mining, unless scientific research purposes are involved. It thus still remains to be seen what the impact of the exceptions will be in practice.

A similar consideration can be made for other particularities of the Directive, such as the scope of the concepts "research organisations" and "cultural heritage institutions" as well as the definition of "online content-sharing service providers" and their duties under the Directive. While the use of protected content by online content-sharing service providers seems to have been restricted quite severely, the impact on data sharing should not necessarily be exaggerated, given the exceptions that are foreseen for newly established online content-sharing service providers, the exclusion of certain services (such as scientific repositories) and the fact that online content-sharing service providers are not subject to a general monitoring obligation. In the future, it will thus be most interesting to follow-up on the impact generated by the Copyright DSM Directive as regards EU data access and data sharing practices. This impact will become clearer as of 7 June 2021, when all Member States will need to have transposed the Directive.

3.1.7 The Trade Secrets Directive

3.1.7.1 Short summary

Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (**Trade Secrets Directive**) is a recent initiative that sets out rules on the protection against unlawful conduct pertaining to the "unlawful acquisition, use and disclosure of trade secrets" (Article 1).

Article 2 of the Directive defines a trade secret as information which meets all of the following requirements:

1. it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
2. it has commercial value because it is secret;
3. it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

It is worth mentioning that a trade secrets are not generally considered to be intellectual property rights. This is because trade secrets do not confer any monopoly rights over the information. Anyone is free to use and share the information covered by the trade secret as long as they do not take it from the trade secret holder through dishonest means. Thus, anyone is free to develop the same information independently (and then use it or share it freely), and reverse engineering (dismantling an apparatus to see how it works) is generally considered a legitimate way of acquiring the information covered by the trade secret.

3.1.7.2 Objectives in relation to data sharing

The purpose of the Trade Secrets Directive is to promote the creation and sharing of information and knowledge, by protecting those who invest in research against dishonest acts such as spying and contract breaching. This allows a trade secret holder to share this type of information while offering him legal protection against the unlawful sharing of information. That being said, with or without this Directive, sharing will not take place if the trade secret holder is not willing to share the information unless, of course, there is a legal obligation to share it.

As such, the Directive does not relate directly to the sharing of data. Data can conceptually however qualify as "information" that satisfies the definition of a trade secret. If such data is shared with too many third parties, it would likely no longer satisfy the requirements of the definition, notably that it is 'not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question'. In that case, it would no longer benefit from the protection provided by the Directive. Whether this is the case or not is a factual question, that will hinge on – among other points – the interpretation given to the 'circles that normally deal with the kind of information in question', i.e. the question of whether the data sharing is sufficiently broad for this requirement to no longer be met.

Inversely, a trade secret can be shared lawfully with third parties and remain a trade secret, if it is shared in such a way that it is protected against becoming generally known (e.g. under a non-disclosure agreement, or using technical measures such as access controls or encryption), and provided that the sharing method does not undermine any reasonable steps taken to maintain its secrecy.

Trade secrets have an important role in protecting the exchange of knowledge between businesses, but this needs to be kept confidential. The sharing of information that is considered as a trade secret, without the consent of the trade secret holder, may give rise to an obligation to compensate the trade secret holder for the damages caused.

The Directive never requires or prohibits data sharing; the trade secret holder always has the power to decide. Nonetheless, the Directive could impact which decision the trade secret holder makes, and the conditions under which such sharing would happen, since an inappropriate sharing decision could imply that the data no longer qualifies as a trade secret.

The Trade Secrets Directive would not apply to information which must be shared by virtue of a legal act in the public interest.

3.1.7.3 Parties targeted or affected

The Directive applies to any legal or natural person, provided that they hold or receive information that can be qualified as a trade secret. This means that any economic sector and any business, irrespective of the size and sector, may benefit from the legal protection the Directive offers against the unlawful acquisition, use or disclosure of trade secrets. Due to its lack of formalities – meaning that there is no need to undergo any registration process in order to qualify information as a trade secret - the Directive is deemed as particularly beneficial for SMEs and research institutions, who would perhaps otherwise struggle to make the investments in order to obtain other forms of protection .

3.1.7.4 Data targeted or affected

The Directive protects information which is commercially valuable for an enterprise, undisclosed and intended to remain confidential.

Knowhow such as business information (e.g. an advanced customer list, results of a study, product development roadmaps, marketing plans) and technical information (e.g. a manufacturing process, recipe, software or a chemical compound) that is considered to have a commercial value can be an example of a trade secret if it meets the requirements of the Directive.

3.1.7.5 Short assessment of its impact

To be noted, trade secrets were already protected though national law in all Member States. However, the protection was not consistent across the Union, and in many cases the requirements of protection, and even the definition of trade secrets, was opaque. The Trade Secrets Directive harmonised the legal framework. Trade secrets law offers protection of legitimate business interests. Offering automatic and harmonised legal protection against unlawful disclosure fosters an environment where a creator can more readily transform the effort invested into business competitiveness and innovation-related performance, and fosters business research and development, while decreasing business risks.

The Directive prevents employees or business partners from sharing data that was passed to them by the trade secret holder. However, for information to qualify as a trade secret, one must comply with the rather strict requirements of the Directive. In addition, it should be stressed that protection only exists where a dishonest behaviour takes place. Moreover, the Directive does not affect transparency or regulatory obligations imposing the disclosure of data, meaning that a company may be obliged by applicable legislation to divulge information for public policy objectives, such as obligations applicable to the chemical and pharmaceutical sector. Finally, journalists remain free to investigate and divulge information on companies' practices and business affairs and the Directive does not impede whistleblowing activities.

By protecting the trade secret holder against the unauthorised disclosure of the trade secret, the Directive promotes the sharing of the information in question within trusted partners, as creators, inventors and entrepreneurs will be more confident that recipients of information will not disclose it to third parties. This is in particular important to promote collaborative research between companies and entities having different areas of expertise. The harmonisation, and clarification, of trade secret law across the Union, contributes to facilitate cross-border research.

In summary, the Trade Secrets Directive provides accessible protection against certain unlawful conduct and is conducive to supporting the development of secure data sharing practices in order to avoid inappropriately broad dissemination of commercially valuable secret information.

3.1.8 The Software Directive

3.1.8.1 Short summary

The Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (**Software Directive**) sets outs rules to protect computer programs as literary works under copyright law. In practical terms, it cements the common understanding that computer programmes can enjoy copyright protections under conditions which are largely comparable to those of other types of intellectual works.

3.1.8.2 Objectives in relation to data sharing

The Software Directive aims to protect computer programs under copyright law as literary works. As such, the Directive offers copyright protection to the expression in any form of a computer program that is original. To this end, the Directive awards exclusive rights to the rightholders (such as the right to reproduction, translation, adaptation, alteration and distribution of the computer program…), that are mirrored by restricted acts. The Directive includes exceptions to these restricted acts and furthermore requires Member States to provide appropriate remedies against acts of possessing or circulating infringing copies of computer programs and acts of possessing or circulating means to facilitate the unauthorised removal or circumvention of technical devices applied to protect a computer program.

As such, the Directive focuses on ensuring protections for computer programs; not on data sharing. None the less, there is a data sharing aspect which is contained in the Directive, notably in relation to interoperability. The function of a computer program is to communicate and work together with other components of a computer system and with users. This requires a logical and (where appropriate) physical interconnection and interaction. This functional interconnection and interaction are generally known as 'interoperability', namely the ability to exchange information and to mutually use the information which has been exchanged.

Given that computer program's interoperability allows for the sharing of data between different devices, entities or databases, computer programs are of key importance in a data sharing economy and, more broadly, are fundamental to the Community's industrial advancement. For this reason, the Directive contains provisions which do not require the sharing of computer programs or their source code in their entirety as such, but which allow decompilation of software – i.e. the automated recreation of the human readable source code behind a computer program – when decompilation is necessary to enable interoperability.

More formally, Article 6 allows decompilation without the authorisation of the rightholder when this is "indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

1. those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so;
2. the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and

3. those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.

The Software Directive therefore contains an indirect incentive to sharing data in relation to the software, namely "information necessary to achieve interoperability": by making this information available, decompilation of the software is no longer lawful, or at least not authorised by the Directive.

3.1.8.3 Parties targeted or affected

The Software Directive offers protection to all natural or legal persons eligible under national copyright legislation as applied to literary work. The beneficiary of such protection will in first instance be the author(s) of the computer program. The author of a computer program is the natural person or group of natural persons who has created the program or, where the legislation of the Member State permits, the legal person designated as the rightholder by that legislation. The author of a computer program may however decide to transfer some or all exclusive rights to another natural or legal person that will then act as the rightholder.

3.1.8.4 Data targeted or affected

The Software Directive applies to the expression in any form of a computer program that is original. The term computer program includes programs that are incorporated into hardware and includes preparatory design material that has the nature for a computer program to result from it at a later stage. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under the Software Directive.

As explained above, the data incentivised for sharing is not so much the software in its entirety, but rather the information required to enable interoperability.

3.1.8.5 Short assessment of its impact

The Software Directive harmonises the protection of computer programs, in order to mitigate any direct and negative effects that differences in the legal protection of Member States have on the functioning of the internal market as regards computer programs. The Directive has a broad scope of harmonisation, since it describes who and what should be protected under copyright law as literary works, which exclusive rights the protected persons should be able to rely in order to authorise or prohibit certain acts and for how long the protection should apply.

Despite this principal focus on protecting creative works, the 'decompilation exception' shows that the Software Directive has taken into account the enormous importance of data sharing in modern society by providing an exception in order to achieve interoperability, and consequently facilitate easy data exchange between different software programs.

Some caveats apply to this general principle. First of all, as underlined above the 'data sharing' aspect does not relate to any obligation to share data processed via specific software, nor to the software itself (either in source code or object code form). It only relates to the information required to enable interoperability – and thus data exchange – between programs. Sharing of raw data (data sets used by the software or the software itself) is out of scope.

Secondly and likely more importantly, the decompilation exception and its impact have changed substantially in the past few years. When the Directive was adopted in 2009, the software industry

very much still relied on a deployment model, where licenses to individual instances of software were purchased and installed locally. In that model, an approach that focused on decompilation made logical sense, since interfaces needed to be built into or attached to pre-existing software. Ten years later however, cloud computing dominates many segments of the software industry – or perhaps more accurate the software service industry. In this model, significantly less software or none at all is locally installed, and decompilation is therefore simply not a practical option: when software operates remotely as a service, a user has no practical option to decompile it, since little to no code is exposed. Instead, the emphasis of the market has shifted towards APIs (application programming interfaces), small software services that can be used to open up data or services within a software package, including in the cloud. This approach can be seen in e.g. the most recent reworking of the PSI Directive (focusing on 'dynamic data' made available via APIs). Thus, the interoperability objective and focus on enabling data sharing has remained – and has a ten-year tradition in the Software Directive – although its emanations in recent legislation have changed shape substantially.

3.1.9 The Digital Content Directive

3.1.9.1 Short summary

Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 (**Digital Content Directive**) regulates certain aspects concerning contracts for the supply of digital content (goods) and digital services. Member States have until 1 July 2021 to transpose this Directive into national law.

The purpose of the Digital Content Directive is to lay down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content (goods) or digital services. In this regard, the consumer is better protected as the burden of proof is in many instances on the trader.

The Directive can be considered an extension of traditional consumer protection law, clarifying that (and how) these protections apply in an electronic environment and to electronic data and services. For instance, the Digital Content Directive contains rules on:

- the conformity of digital content or a digital service with the contract,
- remedies in the event of a lack of such conformity or a failure to supply, and the modalities for the exercise of those remedies, and;
- the modification of digital content or a digital service.

However, it is worth noting that:

- Member States remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled, and;
- some contracts are excluded from the scope of this directive, such as contracts relating to software offered by the trader under a free and open-source license, but also the supply of digital content where the digital content is made available to the general public other than by signal transmission as a part of a performance or event, such as digital cinematographic projections.

3.1.9.2 Objectives in relation to data sharing

With regard to data sharing, the Directive contains no explicit objectives. Rather, it contains a number of obligations that are indirectly conducive to supporting data sharing. Specifically, Article 7 of the Directive contains a series of subjective requirements for conformity, requiring digital content or digital services to:

1. be of the description, quantity and quality, and possess the functionality, compatibility, interoperability and other features, as required by the contract (interoperability being defined *"the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used"*);
2. be fit for any particular purpose for which the consumer requires it and which the consumer made known to the trader at the latest at the time of the conclusion of the contract, and in respect of which the trader has given acceptance;
3. be supplied with all accessories, instructions, including on installation, and customer assistance as required by the contract and;
4. be updated as stipulated by the contract.

Thus, interoperability – and thus the ability to move data to another system, a prerequisite for data sharing – is to some extent regulated, as is the right to obtain the most current version of data available.

3.1.9.3 Parties targeted or affected

As the Digital Content Directive has only recently been adopted, it is still unclear which parties will be most affected in practice for the time being. However, it seems that the provisions of this Directive are expected to affect many parties, in particular traders, meaning any natural or legal person, irrespective of whether it is privately or publicly owned, acting for professional purposes.

The reason for this expectation is that the Digital Content Directive will apply to any digital contract which is not excluded from the scope of this Directive. Hence, it will apply to any contract where a trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price. Consequently, traders that are expected to be affected are, for example, social media platforms, but also providers of cloud-based services or providers of all kinds of digital entertainment services such as video or music streaming services.

One of its recitals gives the example of a consumer opening a social media account and providing a name and email address. If these data are used for purposes other than solely supplying the digital content or digital service or other than complying with legal requirements, then the consumer provides personal data to the social media provider instead of paying a price. In such case, the social media provider will have to comply with the provisions of the Digital Content Directive. In other words, the Digital Content Directive will apply if the personal data of the consumer are used for marketing purposes.

Consumers making use of the digital content or the digital service will also be affected or rather protected by the provisions of this Directive.

3.1.9.4 Data targeted or affected

The Directive targets digital content, generically defined in the Directive as "data which are produced and supplied in digital form" (Article 2(1)). Digital services are defined as services "that allow the consumer to create, process, store or access data in digital form or that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service" (Article 2(2)). In this digital day and age, business models exist in which the digital content or digital service is seemingly free of charge. In recital 24, the Digital Content Directive confirms the existence of the business model where consumers do not pay a price but provide personal data to the trader. Recital 24 clarifies that the directive should also apply to those kinds of contracts, as the consumer should be protected and entitled to contractual remedies. In such case, the trader also must comply with the GDPR.

In relation to digital contracts, the Digital Content Directive stipulates that the price paid by the consumer means either money or a digital representation of value that is due in exchange for the supply of digital content or a digital service. In other words, if the consumer shares his or her personal data with the trader in exchange for digital content or a digital service, then the provisions of this Digital Content Directive will apply.

3.1.9.5 Short assessment of its impact

As the Digital Content Directive is only recently adopted and remains to be transposed by the national Member States, the real impact in practice is still to be seen.

It is worth mentioning that the definitions of 'digital content' and 'digital service' are rather broad. As contracts are increasingly being digitised, this Directive is likely to play an important role, now and in the future, even though some contracts are explicitly excluded from the scope of the Digital Content Directive. In particular, its emphasis on availability, interoperability and currency (meaning that the most current version of data must be available) can be influential in shaping future legislative initiatives.

3.2 Non-legislative normative documents with general or horizontal application

3.2.1 Non-legislative normative document: Recommendation of the European Commission on the preservation and access of scientific information

3.2.1.1 Short summary

The Commission Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information (**Recommendation on scientific information**) obliges Member States to set and implement clear policies (as detailed in national action plans) relating to the exchange of scientific information.

3.2.1.2 Objectives in relation to data sharing

The Recommendation on scientific information stretches that preservation of scientific research results is in the public interest and the sharing of such information is therefore key in this Recommendation. In order to meet this objective, the Recommendation strongly recommends and encourages Member States to set and implement clear policies for inter alia the:

- dissemination of and open access to scientific publications resulting from publicly funded research;
- management of research data resulting from publicly funded research, including open access;
- reinforcement of the preservation and re-use of scientific information (publications, data sets and other research outputs).

3.2.1.3 Parties targeted or affected

The Recommendation does not explicitly state which parties will be subject to the policies drafted by the Member States, since it is up to Member States to decide upon that. However, it is clear that the policies will apply to players active in the field of scientific research.

3.2.1.4 Data targeted or affected

The Recommendation applies to scientific information in general, such as information extracting from scientific publications, research data, etc.

3.2.1.5 Short assessment of its impact

Open access to scientific information will help to enhance quality, to reduce the need for unnecessary duplication of research, to speed up scientific progress, will help to combat scientific fraud, and can overall favour economic growth and innovation.

The Recommendation recognizes the importance of licensing solutions, which should aim at facilitating the dissemination and re-use of scientific publications and the Recommendation even states that the policies that should be drafted by the Member States should provide for appropriate licensing.

However, this leaves a significant margin of national policy for Member States, supporting flexibility but also potentially leading to fragmentation. As an example, it remains unclear how the sharing of scientific information will take place, for example, from databases with data spread across different countries to which different research institutes have collaborated, located in different countries.

3.3 Sector-specific rules

3.3.1 Public Sector Information Directive ('PSI Directive' or 'Open Data Directive')

3.3.1.1 Short summary

Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (the **PSI Directive or Open Data Directive**) entered into force on 16 July 2019 and replaces Directive 2003/98/EC as of 17 July 2021, which was amended by Directive 2013/37/EU.

3.3.1.2 Objectives in relation to data sharing

The Open Data Directive is based on the general principle that public-sector information held by public-sector bodies or public undertakings, and of publicly funded research data should be reusable for commercial and non-commercial purposes, free of charge. Public sector bodies are furthermore required to make dynamic data available for re-use immediately after collection, via suitable Application Programming Interfaces (APIs) and, where relevant, as a bulk download. The concept of 'dynamic data' was newly introduced by this Directive and is defined as "documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence" (Article 2.8). This shows that, for public sector information too, there is a shift towards 'data as a service', rather than merely as static downloads.

Moreover, the Directive also introduces the concept of "high value datasets", defined as documents the re-use of which is associated with important benefits for the society and economy. They are subject to a separate set of rules ensuring their availability free of charge, in machine readable formats, provided via APIs and, where relevant, as bulk download. The sharing of such datasets is highly stimulated by the Directive.

As a consequence, the Directive aims at boosting the socio-economic potential of public-sector information and makes this information more easily available for companies by increasing the supply of dynamic data and of datasets with a particularly high economic impact, while at the same time promoting competition and transparency in the information market.

3.3.1.3 Parties targeted or affected

The Open Data Directive applies public sector bodies and public undertakings (as defined in Article 2), as well as to research organisations. Universities could also fall under the scope of the Directive, depending on their status under national law (as public sector bodies, public undertakings or private sector bodies) and their activities (notably whether they qualify as research organisations).

The available information could be re-used by any type of users, such as businesses, other public sector bodies or public undertakings, researchers and individuals.

3.3.1.4 Data targeted or affected

The Directive applies in principle to all accessible public-sector information such as geographical, land registry, statistical or legal information held by public-sector bodies and some public undertakings, and to accessible publicly funded research data.

The Directive also provides for a special legal regime when it comes to so-called high-value datasets. Annex I of the Directive defines the following categories of high-value datasets: (a) geospatial datasets, (b) datasets consisting of information regarding earth observation and environment, (c) meteorological datasets, (d) statistical datasets, (e) datasets consisting of information regarding companies and company ownership and, (f) datasets consisting of information regarding mobility.

The Directive covers all types of documents containing such information, including written texts, databases, audio files and film fragments.

However, a few situations are exempted from the scope of the Directive (Article 1.2). The Directive does not apply to (a) documents for which third parties hold intellectual property rights, (b) documents whose access is excluded or restricted on the virtue of a national access regime or on the grounds of sensitive critical infrastructure protection, (c) documents whose supply falls outside the scope of the public task of a public-sector body or outside the scope of provision of services in the general interest of a public undertaking, (d) documents related to the activities of a public undertaking directly exposed to competition and therefore not subject to procurement rules under Article 34 of Directive 2014/25/EU and, (e) other documents referred to in Article 1.2 of the Directive.

3.3.1.5 Short assessment of its impact

The Directive modernises the existing PSI framework in many ways, including most notably by expanding the stakeholders and the data covered, by introducing a specific focus on high value datasets, and by including dynamic data and APIs within its scope. When it comes to research data, Member States are required to support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available ('open access policies'), following the principle of 'open by default' and compatible with the FAIR principle (i.e. ensuring that research data are findable, accessible, interoperable and re-usable). In all, the Directive should have a strongly beneficial impact on data sharing in the sectors covered.

3.3.2 The MIFID framework: MIFID II and MIFIR

3.3.2.1 Short summary

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (**MIFID II**) lays down, among other things, rules for financial institutions which provide investment and/or ancillary services to regulate financial markets. MiFID II is the successor to the MiFID I Directive. The Regulation (EU) No 600/2014 of 15 May 2014 on markets in financial instruments (**MIFIR**) is concerned with regulating the operation of these trading venues and the processes, systems and governance measures adopted by market participants.

3.3.2.2 Objectives in relation to data sharing

The objective of the MIFID framework is to strengthen the framework for the regulation of markets in financial instruments, including where trading in such markets takes place over-the-counter (OTC), in order to increase transparency, better protect investors, reinforce confidence, address unregulated areas, which have been exposed by the financial crisis.

While the MIFID2 provides the framework and the regulation of the financial market, the MIFIR establishes uniform requirements concerning the disclosure of trade data to the public, and reporting transactions to the competent authorities.

3.3.2.3 Parties targeted or affected

The Parties targeted or affected by the transparency requirement are trading venues and investment firms, which provide the information, and investors who benefit from it.

The MIFID2 organises the actors having the abilities to provide this information and requires their registration for authorisation by a competent authority. The Directives considers the following types of providers:

- approved publication arrangement (APA): a provider authorised to provide the service of publishing trade reports on behalf of investment firms;
- consolidated tape provider (CTP): a provider authorised to provide the service of collecting trade reports for financial instruments and consolidating them into a continuous electronic live data stream providing price and volume data per financial instrument and;
- approved reporting mechanism (ARM): provider authorised to provide the service of reporting details of transactions to competent authorities or to ESMA on behalf of investment firms.

3.3.2.4 Data targeted or affected

The information reported entails the complete and accurate details of transactions in financial instruments, as quickly as possible.

3.3.2.5 Short assessment of its impact

MIFID II and MIFIR aim to ensure fairer, safer and more efficient markets, as well as greater transparency for all participants by harmonising and streamlining the information which is available to them. The amount of information on transactions has thereby increased in practice. Overall, the

protection of individual investors has been improved. For market operators, substantial efforts in compliance preparation were however needed, and some financial instruments are unavailable on European markets due to a lack of available information on their characteristics.

3.3.3 The Payment Services Directive 2 (PSD2)

3.3.3.1 Short summary

Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (**PSD2,** the successor to PSD1) introduces enhanced security measures to be implemented by all payment service providers. Furthermore, it introduces new categories of service providers (account servicing payment service providers, payment initiation service providers, and account information service providers) who are able under certain conditions to obtain access to certain account information from payment service providers (i.e. a form of data sharing which is mandatory once the customer has authorised it).

3.3.3.2 Objectives in relation to data sharing

The Directive establishes rules to provide more flexibility and freedom to customers regarding their payment data. They are able to make their data available to third party service providers – who must also meet supervisory and security requirements - while maintaining the confidentiality of these data.

Customers decide for themselves whether they want to give these third parties access to their payment accounts, and they can refuse any request for permission from a third party if they wish to do so. This means that, in terms of data sharing, customers retain complete control. Data may only be shared on their request. Inversely, payment institutions or other targeted institutions may not refuse to share data with these third parties once the transfer has been authorised by the customers.

PSD2 also reinforces the obligation to keep customers' financial data confidential. The Directive concentrates heavily on strong customer authentication (SCA). Banks must implement appropriate security measures to ensure the confidentiality of their data. Here again, the position of the customer is key.

3.3.3.3 Parties targeted or affected

Due to PSD2, bank customers – including both individual customers and businesses – can exercise control over the transmission of their financial transaction data and may conduct their finances through third-party providers.

3.3.3.4 Data targeted or affected

The Directive sets out rules on the transmission and use of financial (transaction) data.

3.3.3.5 Short assessment of its impact

The Directive aims to increased competition in the financial sector and more protection of customers' accounts. To achieve this goal, PSD2 establishes rules that will ensure transparency towards customers.

Banks are forced to share their customers' financial transaction data on their request. The banks' monopoly on their customers' data is therefore eliminated, or at least significantly reduced. Third-party providers may initiate payments for the customers directly from their bank account, as banks

are forced to open access to their customers' accounts to third-party providers via application programme interfaces (APIs). In addition, banks must implement appropriate security measures to keep customers' data confidential. This means that banks must convince their customers to use two-stage identity verification. The European Bank Agency (EBA) drafted technical standards covering various technical issues, particularly the issue of SCA.[52] SCA is an authentication based on the use of two or more elements categorised as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

The implementation of these rules should eventually lead to a better integrated internal market for electronic payments within the European Union, and above all more innovation and competition.

Since the decision-making power to share payment data lies entirely with the customer and since payment service providers must ensure the confidentiality of such data, the impact of this legislation is largely limited to the relationship between the customer and his or her payment service provider.

3.3.4 ePrivacy Directive and the European Electronic Communication Code

3.3.4.1 Short summary

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (**ePrivacy Directive**), as amended by Directive 2009/136/EC of 25 November 2009 (colloquially referred as the **Cookies Directive**) provides the basic legal framework for data protection in electronic communications. Its scope is not limited to traditional telecommunications (i.e. phone-based services), as the Directive applies to "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service".

While this excludes broadcasting services where the exchanged information cannot be related to the identifiable subscriber or user receiving the information, it does include some online communications such as website usage. Automated machine to machine communications (including most IoT applications) are however out of scope; this is a potential gap that might be corrected through a future ePrivacy Regulation, as will be discussed in the section directly below.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (**European Electronic Communication Code**) lays down the general updated EU telecom rules; the Code also defines the common concepts used by the ePrivacy Directive.

The Directive contains high level provisions requiring such communications to be appropriately secured, and in relation to the confidentiality of electronic communications. In addition, it contains rules relating to location data and other traffic data, restricting the conditions under which such data can be collected and used; these rules are of particular relevance for the present report. Other

[52] https://eba.europa.eu/-/eba-provides-clarity-to-market-participants-for-the-implementation-of-the-technical-standards-on-strong-customer-authentication-and-common-and-secure-

provisions relate to traditional communications issues (such as caller identification, unsolicited communications and subscriber directories) which will not be discussed in this report.

3.3.4.2 Objectives in relation to data sharing

Like the GDPR, the Directive focuses (among other topics) on ensuring that the confidentiality of electronic communications is appropriately ensured. As a result, data sharing is not a priority of the Directive. None the less, location data and traffic data are of significant importance to the data economy, as key inputs for the creation of innovative services, and for this reason the constraints on collecting and sharing such data are highly relevant.

Traffic data is defined in Article 2 of the Directive as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". It is a very broad data category comprising most types of metadata that are required to connect communications or enable transactions between devices. Location data is a specific kind of traffic data, which indicates the geographic position of the terminal equipment of a user. Given the importance of geolocation in the data economy (e.g. to enable localised services), access to such information is both economically important and privacy sensitive.

The Directive imposes strict rules for such data types. Traffic data may only be retained by the provider of a public communications network or publicly available electronic communications service for as long as required to enable the service or billing; thereafter it must be deleted or anonymised. Any other use (notably for added value services) requires the prior informed consent of the users involved, which must be revocable at any time. Location data other than traffic data similarly requires either consent or anonymisation.

Collectively, the rules imply that such data cannot be shared with third parties by providers of a public communications network or publicly available electronic communications service, with the exception of third parties that they've authorised to engage in processing activities that the service providers themselves are already permitted to engage in.

3.3.4.3 Parties targeted or affected

Crucially, the Directive targets only the providers of a public communications network or publicly available electronic communications service. This concept is defined as a part of the broader telecommunications framework (now integrated in the European Electronic Communication Code), and excludes information society services, as defined in the eCommerce Directive, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. In other words, the parties targeted include principally traditional telecommunications service providers, but not online service providers offering functionally comparable services, nor IoT applications providers. The elevated level of protection of traffic data and location data as specified in the Directive is therefore limited to those stakeholders; other service providers collecting, processing or sharing traffic data and location must instead abide by the GDPR.

3.3.4.4 Data targeted or affected

Beyond the contents of electronic communications themselves, the principal data targeted are traffic data and location data as described above.

3.3.4.5 Short assessment of its impact

The ePrivacy Directive has had a significant impact on data sharing (and more broadly data collection and data processing) in the telecommunications industry, since processing of communications contents, traffic data and location data are generally only permissible if required for the provision and management of the service, or based on the consent of the subscriber. This provides an admittedly high level of protection for potentially very sensitive communication, but also acts as a clear disincentive for data sharing. As underlined above, there is a consistency challenge due to the scoping of the Directive, which targets only traditional telecommunications services but excludes most types of IoT services, which are critical e.g. in the context of smart mobility, smart cities, modern health care, etc. The latter would be subject to the GDPR, leaving potentially more margin for processing without the prior consent of the user. This is one of the problems that the proposal for an ePrivacy Regulation endeavoured to correct, as will be described directly below.

3.3.5 Prospective assessment: the proposal for an ePrivacy Regulation

3.3.5.1 Short summary

A proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (**proposal for an ePrivacy Regulation**) comprises rules for (new) electronic communication service providers and (traditional) telecom providers, i.e. providers of electronic communication networks and services. While retaining the major principles of the ePrivacy Directive, the proposal aims to expand the scope of the ePrivacy framework by also including online communications service providers (such as WhatsApp, Facebook Messenger and Skype), as well as machine to machine communications and thus IoT services. Furthermore, the proposal makes a clearer distinction between communications content and metadata in general, the latter of which would comprise both the older notions of traffic data and location data.

3.3.5.2 Objectives in relation to data sharing

As with the existing ePrivacy Directive, the aim of the proposal is to maintain confidentiality of electronic communications of users. Providers of electronic communication networks and services are not allowed to share electronic communications metadata with third parties without the consent of users, unless the metadata is made anonymous or unless the data is needed for billing purposes.

3.3.5.3 Parties targeted or affected

The rules of the proposal for an ePrivacy Regulation apply to providers of electronic communication networks and services, now expanded to also include providers of information society services if they enable electronic communication.

3.3.5.4 Data targeted or affected

The confidentiality of communications applies to the content of the communication as well as to the metadata. Metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.

3.3.5.5 Short assessment of its impact

Given that the text is still a proposal, its impact is highly limited at this stage.

3.3.6 Commission delegated Regulation No 886/2013 on road safety-related minimum universal traffic data

3.3.6.1 Short summary

The Commission Delegated Regulation of 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users (**Commission delegated Regulation No 886/2013**), establishes the specifications necessary to ensure compatibility, interoperability and continuity for the deployment and operational use of data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users on EU level.

3.3.6.2 Objectives in relation to data sharing

The primary objective of this Commission Delegated Regulation is to exchange and reuse road safety-related traffic data to guarantee traffic safety within the EU. Citizens must be properly informed about traffic incidents and situations.

Data must be made available via the same format to achieve compatibility, interoperability and continuity. An EU harmonised profile has been created for the purpose of making road safety-related traffic data available in the same format.[53]

3.3.6.3 Parties targeted or affected

Public and/or private road operators and/or service providers should detect and identify events and conditions and should collect relevant road safety-related traffic data. They should make these data accessible through individual access points or they should make sure that they are accessible through national access points set up and managed by the Member States, where it will be accessible for reuse. Data must be accessible for any driver benefiting from road safety-related minimum universal traffic information services.

3.3.6.4 Data targeted or affected

The Commission delegated Regulation No 886/2013 refers to the concept of road safety-related minimum universal traffic information. This notion includes all extracted, aggregated and processed road safety-related traffic data, offered by public and/or private road operators and/or service providers to end users through any delivery channels.

It concerns information such as the location of an event or a condition, the category of an event or a condition, and, where appropriate, short description of it (i.e. (a) temporary slippery road; (b) animal, people, obstacles, debris on the road; (c) unprotected accident area; (d) short-term road works; (e)

[53] https://ec.europa.eu/transport/themes/its/road/action_plan/traffic-information_en.

reduced visibility; (f) wrong-way driver; (g) unmanaged blockage of a road; (h) exceptional weather conditions) and driving behaviour advice.

The Commission delegated Regulation No 886/2013 explicitly mentions that the publicity of these data must occur in accordance with data protection requirements when the data involves personal data, such as for example an end-user's geolocation.

3.3.6.5 Short assessment of its impact

The Commission delegated Regulation helps to informing citizens about safety-related traffic events or conditions. This can be achieved by using the same data format, providing all citizens with the same information. This initiative is likely contribute to the overall road safety in the EU and will reduce the number of accidents and incidents.

From a strategic perspective, the Regulation is particularly notable due to its identification of a specific technical standard to be followed (the DATEX II (CEN/TS 16157) format, to ensure compatibility, interoperability and continuity for the deployment and operational use of Intelligent Transport Systems (ITS) for the provision of EU-wide safety related traffic information (SRTI) and real-time traffic information (RTTI) services. While this is arguably a barrier to innovation (since all data must fit into the existing standard), it does support data sharing. In addition, the risk is minimised since the referenced standard is an EU harmonized profile, allowing DATEX II users to customize their implementations according to their own requirements, whilst keeping interoperability on common parts (publications, operating modes) with other users. This can be considered a best practice to facilitate data sharing.

3.3.7 Vehicle Repair and Maintenance Information (RMI) and Vehicle Emissions Regulation

3.3.7.1 Short summary

Regulation No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (**Vehicle Emissions Regulation**) regulates vehicle emissions for small passenger and commercial motor vehicles and lays down rules to ensure that independent operators have access to vehicle repair and maintenance information (RMI).[54]

As from 1 September 2020, the Vehicle Emissions Regulation will be amended by Regulation 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 of systems, components and separate technical

[54] Note that similar requirements are laid down for heavy duty vehicles in Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC.

units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

3.3.7.2 Objectives in relation to data sharing

The aim of the Vehicle Emissions Regulation is to ensure that EU car manufacturers provide unrestricted and standardised access to vehicle RMI to independent operators with the purpose of preventing that manufacturers would discriminate against independent operators. It thus enables competition and avoids lock-in.

3.3.7.3 Parties targeted or affected

The Regulation obliges EU car manufacturers to share information with independent operators. Independent operators are defined as undertakings other than authorised dealers and repairers which are involved in the repair and maintenance of motor vehicles.

Examples hereof are repairers, manufacturers or distributors of repair equipment, tools or spare parts, publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment for alternative fuel vehicles.

3.3.7.4 Data targeted or affected

The data concerned consists of vehicle generated data and/or operating data. This implies the following information: (a) an unequivocal vehicle identification; (b) service handbooks; (c) technical manuals; (d) component and diagnosis information (such as minimum and maximum theoretical values for measurements); (e) wiring diagrams; (f) diagnostic trouble codes (including manufacturer specific codes); (g) the software calibration identification number applicable to a vehicle type; (h) information provided concerning, and delivered by means of, proprietary tools and equipment; and (i) data record information and two-directional monitoring and test data.

Data imported by vehicle users (such as mobile phone contact lists and selected destinations for navigation) and data received from external sources (such as information transmitted by roadside units and other vehicles or vulnerable road users) is excluded.[55]

3.3.7.5 Short assessment of its impact

The Commission published a report in 2016 on the operation of the system of access to vehicle RMI. The report assessed the operation of the system of access to RMI in the EU, as well as its effects on competition, the Internal Market, environment and safety. However, the report shows that despite the progress achieved, there remain difficulties which hinder the overall functioning of the system of access to vehicle RMI.[56] Furthermore, the impact of the RMI regulation is limited due to the fact that it is not an instrument that focuses on enabling innovation through data sharing: the purpose of the regulation is to allow maintenance and to protect the environment; not to allow any kind of

[55] European Automobile Manufacturers Association, *ACEA Position Papers, Access to vehicle data for third-party services*, https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf.

[56] Report of the European Commission, on the operation of the system of access to vehicle repair and maintenance information established by Regulation (EC) No 715/2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0782&from=nl.

innovation by making all vehicle information accessible to third parties. Thus, for some added value services, car manufacturers retain a relative monopoly, in the sense that third parties will need to contact them to obtain applicable terms and conditions for data sharing.

3.3.8 REACH Regulation

3.3.8.1 Short summary

Regulation No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (**REACH Regulation**) legislates the registration, evaluation, authorisation and restriction of chemicals. In principle, REACH applies to all chemical substances, not only industrial or high-risk ones. It has applied in the EU since 1 June 2007.

At the highest level, REACH strengthens the responsibilities of industry stakeholders, both for assessing and managing risks, and for providing appropriate safety information for users of chemicals. As such, it requires new forms of cooperation among companies, including by enhancing communication – i.e. sharing data – along the supply chain. The principal REACH Regulation is backed by extensive supporting and implementing legislation[57], including on data sharing (Commission Implementing Regulations 2016/9 and 2019/1692).

3.3.8.2 Objectives in relation to data sharing

One of the fundamentals aspects of the REACH Regulation is to share information about substances manufactured, imported, placed on the market and used in the EU with the purpose of ensuring a high level of protection of human health and the environment.

In order to comply with REACH, companies are required to register their chemical substances, in collaboration (including by sharing relevant data) with other companies who are registering the same substance. The European Chemicals Agency (ECHA) receives and evaluates registrations for their compliance, and EU Member States evaluate selected substances to clarify initial concerns for human health or for the environment. Authorities and ECHA's scientific committees assess whether the risks of substances can be managed. Thus, substantial data exchange is required in order to prevent tests being duplicated.

3.3.8.3 Parties targeted or affected

The obligations of the REACH Regulation apply to manufacturers, importers and downstream users of chemical substances on their own, in mixtures or in articles. It impacts on a wide range of companies across many sectors beyond the chemical industry. Obligations also apply to public authorities.

[57] See https://ec.europa.eu/growth/sectors/chemicals/legislation_en for a complete overview.

3.3.8.4 Data targeted or affected

Principally, REACH requires data to be collected and shared in relation to the risks linked to chemical substances produced and marketed in the EU. This data generally takes the form of studies. As highlighted above, a joint submission of data and data-sharing can be mandatory under REACH in situations where multiple companies are required to submit a registration related to the same chemical.

Data sharing is in practice done in Substance Information Exchange Fora (SIEF) for substances already on the market when REACH entered into force (the so-called phase-in substances) or through the inquiry process for new substances (non-phase-in substances). If the information is not available, potential registrants have to agree who will undertake the necessary testing and ensure that the test is carried out only once.

This process is regulated by Implementing Regulation (EU) 2016/9[58], which requires parties in such a situation to make every effort to reach a data-sharing agreement covering the required information. Mandatory elements of this agreement are regulated (including data items and cost sharing, which must be fair and non-discriminatory). Comprehensive guidance on the data sharing requirements has been made available by ECHA[59].

Registrants must refrain from exchanging information on their market behaviour, in order to mitigate competition issues.

In addition, there are multiple downstream data sharing requirements comprised in REACH:

- Suppliers must provide recipients of hazardous substances or mixtures, PBT[60] /vPvB[61] substances or SVHC[62] substances with safety data sheets containing hazard and risk management information. Safety data sheets may have to include exposure scenarios[63] in an annex.
- Suppliers of articles containing SVHC substances must provide recipients of those articles with sufficient information to allow safe use of the article; they must provide such information to consumers upon request.

An upstream data sharing component was also introduced in REACH: downstream users of chemicals and distributors have to communicate up the supply chain on any risks they encounter, thus enabling registrants to better understand risks and maintain their registrations.

Finally, the REACH Regulation requires large amounts of information on substances to be made publicly available by ECHA, free of charge, including results of studies[64]. In some cases, information submitters may oppose the publication of information due to potential harm to the commercial interests to themselves or any party concerned.

---

[58] Commission Implementing Regulation (EU) 2016/9 of 5 January 2016 on joint submission of data and data-sharing in accordance with Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0009

[59] See https://echa.europa.eu/documents/10162/23036412/guidance_on_data_sharing_en.pdf/545e4463-9e67-43f0-852f-35e70a8ead60

[60] Persistent, bioaccumulative and toxic.

[61] Very persistent and very bioaccumulative.

[62] Substances of very high concern.

[63] The set of conditions, including operational conditions and risk management measures, that describe how the substance is manufactured or used during its lifecycle and how the manufacturer or importer controls, or recommends downstream users to control, exposures of humans and the environment.

[64] Available at https://ec.europa.eu/growth/sectors/chemicals/reach/studies_en

3.3.8.5 Short assessment of its impact

A major reason why the REACH Regulation was drafted was that many substances have been manufactured and placed on the market in Europe for years, without having enough information on the risks and threats they pose to human health and the environment.[65]

The adoption of this Regulation fills these information gaps and aims at ensuring that the manufacturers and importers of substances can assess hazards and risks of the substances, and to identify and implement the risk management measures to protect humans and the environment and recommend them to their downstream users. This contributes to safe handling and reduces the risks imposed to humans and the environment.

Two formal reviews of the REACH Regulation have been conducted by the European Commission, after the first 5 and the first 10 years of operation respectively. The most recent of these, the 2017 REACH Refit evaluation[66], indicated that REACH "has steadily improved as experience was gained. REACH provides a comprehensive data generation and assessment system for chemicals manufactured and used in the EU"[67]; and that "since the 2013 REACH Review, the data sharing process has been further improved, and is the most important contributor to avoiding animal testing"[68]. While non-compliance of registration dossiers was also reported, data aggregation, sharing and dissemination thus generally seems to be satisfactory.

In relation to data sharing, the evaluation report noted that "there has been a continued increase in the information passed through the supply chain, though it needs to be made more efficient (e.g. reduce costs of producing and supplying Safety Data Sheets), especially for SMEs", and that "ECHA has established a user-friendly website enabling stakeholders to easily access the world's largest database on chemicals". The data sharing concerns will likely have been mitigated to some extent, since data collection for the evaluation preceded the entry into application of the aforementioned Implementing Regulation (EU) 2016/9, which governs data sharing in particular.

3.3.9 Energy Framework (Clean Energy for All Europeans Package)

3.3.9.1 Short summary

The Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (**Electricity Directive 2009**) sets out common rules for the generation, transmission, distribution and supply of electricity. A wide range of initiatives has been taken to make consumers an active part of the clean energy transition and help them save more money and energy. However, Europe's energy system is in the middle of a profound change and the EU legislator therefore adopted in May 2019 its Clean energy for all Europeans package, which includes several legislative files. Relevant in the context of this report is the Directive 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU

[65] https://ec.europa.eu/environment/chemicals/reach/reach_en.htm

[66] Available at https://ec.europa.eu/growth/sectors/chemicals/reach/review_en

[67] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:116:FIN

[68] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:58:FIN

(**Electricity Directive 2019**) which sets out (new) common rules for the generation, transmission, distribution and supply of electricity. This Directive enhances the existing rules set out in the Electricity Directive 2009 to even better protect and empower final customers by, among other matters, providing them with transparent information. EU countries have 18 months to transpose the new measures into national law. Until then, the Electricity Directive 2009 will still apply.

Likewise, Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (**Gas Directive**) sets out similar rules pertaining gas. The rules governing gas will be explained in a later version of this report.

3.3.9.2 Objectives in relation to data sharing

Due to the Clean energy for all Europeans package, citizens play a central role in the energy legal acquis. The aim of the energy package is providing transparent information to consumers about their energy consumption. Sharing transparent information with customers about their energy consumption is used as a tool to safeguard consumer protection and to preserve that all consumers in the wider remit of the EU benefit from a competitive and liberalised internal energy market. Accordingly, clear and comprehensible information should be made available to consumers concerning their rights in relation to the energy sector.

For one thing, the Electricity Directive 2019 will improve the information on electricity bills which allows customers to better control their costs while at the same time empowering them to better modulate their energy purchases and participate in demand response schemes.

A prominent example is the introduction and employment of the smart metering system in Article 19 of the Electricity Directive 2019. Member States must inter alia ensure the deployment in their territories of smart metering systems that assist the active participation of customers in the electricity market. A smart metering system enables consumers to provide up-to-date information on their gas/ electricity consumptions (i.e. (near) real time data and interval data). This allows them to manage their energy use and reduce their energy bills. On top of that, Member States must ensure that final customers who have a smart meter installed can request to conclude a dynamic electricity price contract and that they are informed about the existence of such a contract. This again allows consumers to benefit – in an informed manner – from market-based offers.

3.3.9.3 Parties targeted or affected

The energy package regulates the rights and obligations of different stakeholders active in the energy sector, such as the customers (e.g. wholesale customers, final customers, (non-)household-customers), distribution system operators, electricity suppliers etc.

3.3.9.4 Data targeted or affected

Article 23 of the Energy Directive 2019 clarifies that “data” under the Directive shall be understood to include metering and consumption data as well as data required for customer switching, demand response and other services.

3.3.9.5 Short assessment of its impact

Sharing transparent information with customers about their energy consumption is used as a tool to safeguard consumer protection and to preserve that all consumers in the wider remit of the EU benefit from a competitive and liberalised internal energy market. Accordingly, clear and comprehensible information should be made available to consumers concerning their rights in relation to the energy sector.

These rules enable customers to choose in an informed manner a suitable energy provider, since they enable customers to take ownership of their energy transition, benefit from new technologies to reduce their bills and participate actively in the market. This puts an end to estimated bills and create control for customers over their energy consumption or generation.

Under the Electricity Directive, the focus was already on giving consumers a better overview of their energy consumption. However, the new Directive on common rules for the internal market for electricity goes a step further in informing customers and has launched the smart metering system. A smart meter is an electronic device that records consumption of electric energy and natural gas and communicates the information to the energy supplier for monitoring and billing purposes. These new rules outline a comprehensive framework for consumer protection, information and empowerment in the EU electricity sector. They require energy providers to be even more transparent to consumers, and to provide more accurate and detailed information regarding their energy consumption.

For example, the Flemish Regulator for the Electricity and Gas Market ("VREG") carried out an updated cost-benefit analysis and came to the conclusion that, calculated for society as a whole, the roll-out of the smart meter is the right policy decision, but the effects can vary from one customer to another.[69]

In terms of data sharing, the impact of these rules is that energy providers must be fully transparent when it comes to energy consumption data of customers. The impact for customers will be that they have better control their energy consumption and purchases. In view of changing legislation as explained above, it is too early to determine what the actual impact will be.

It is also worth mentioning Articles 23 and 24 of the Electricity Directive 2019. Article 23 lays down the rules on data management. The Article stipulates that Member States or, if applicable, the designated authorities shall specify the rules on the access to data of the final customer by eligible parties in accordance with that Article. Article 24 stipulates that the EC will adopt, by means of implementing acts, interoperability requirements and non-discriminatory and transparent procedures for access to data referred on in Article 23. It is up to Member States to ensure that electricity undertakings apply these requirements and procedures.

[69] https://www.vreg.be/nl/document/rapp-2018-01

3.3.10 Clinical Trial Regulation

3.3.10.1 Short summary

Regulation No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (**Clinical Trial Regulation**) requires (i) consistent rules for conducting clinical trials throughout the EU and (ii) information on the authorisation, conduct and results of each clinical trial carried out in the EU to be publicly available.

3.3.10.2 Objectives in relation to data sharing

Sharing clinical trials information is of paramount importance to this Regulation.

The Regulation desires with its provisions to increase the efficacy of EU clinical trials and to foster innovation and research, while preventing redundancy of clinical trials or duplication of unsuccessful trials. In addition, the Regulation aims to create transparency of clinical trials conducted in the EU. To achieve these goals, the Regulation requires organisations to submit the concerned information to be made public, based on predefined disclosure rules.

3.3.10.3 Parties targeted or affected

Every organisation that conducts a clinical trial in the EU is subject to the provisions of the Regulation.

3.3.10.4 Data targeted or affected

Organisations must submit summary results and clinical study reports of the clinical trials they have conducted in the EU.

Note that the right to information is not absolute and it is subject to exceptions. These exceptions are:

- the protection of personal data;
- the protection of commercially confidential information, in particular taking into account the marketing authorisation status of the medicinal product, unless there is an overriding public interest in disclosure;
- the protection of confidential communication between Member States in preparing their assessment;
- the protection of the supervision of clinical trials by Member States.

3.3.10.5 Short assessment of its impact

In order to create full transparency of clinical trials conducted in the EU, the EU Clinical Trials Register has been created,[70] which contains information on interventional clinical trials on medicines conducted in the EU or the EEA and information about older paediatric trials covered by an EU marketing authorisation.[71] This register also enables users to search for information in the EudraCT database, which is the database used by national medicines regulators for data related to clinical trial

[70] https://www.clinicaltrialsregister.eu/about.html
[71] https://www.ema.europa.eu/en/human-regulatory/research-development/clinical-trials/clinical-trial-regulation

protocols.[72] The European Medicines Agency (EMA) provides guidance on the sharing of clinical trials data, as well as on the EU portal and EU database.[73]

As previously mentioned, the Regulation increases the efficacy of EU clinical trials, fosters innovation and research, and prevents the redundancy of clinical trials or duplication of unsuccessful trials. Moreover, users can very easily search for information via the dedicated portal and database.

According to the EU Clinical Trails Registers website, the Register currently displays 35.890 clinical trials with a EudraCT protocol, of which 5.888 are clinical trials conducted with subjects less than 18 years old.[74] These very high figures show the relevance of the Regulation, as many datasets are freely available.

3.3.11INSPIRE Directive

3.3.11.1 Short summary

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (**INSPIRE Directive**) sets out rules to set up an infrastructure for spatial information. The Directive addresses 34 spatial data themes needed for environmental applications.

3.3.11.2 Objectives in relation to data sharing

The INSPIRE Directive establishes an infrastructure for spatial information in Europe and enables the sharing of environmental spatial information among public sector organisations, facilitates public access to spatial information across the EU and assists in policymaking across boundaries.

3.3.11.3 Parties targeted or affected

The INSPIRE Directive mainly focuses on public authorities but acknowledges that certain relevant spatial datasets and services are held and operated by private third parties. Therefore, private parties may also contribute to the national infrastructures, but this is made subject to strict conditions.

3.3.11.4 Data targeted or affected

The INSPIRE Directive lays down rules to set up an infrastructure for spatial information. Spatial information directly or indirectly refers to a specific location or geographical area and includes information related to transport networks, for the purpose of EU environmental policies. Examples are ground water, transport networks, population, land use and air temperatures.

3.3.11.5 Short assessment of its impact

Each Member State has its own way of describing spatial information, but our environment does not stop at the borders of each Member State. The INSPIRE Directive aims at making spatial or geographical information more accessible and interoperable for a wide range of purposes supporting sustainable development and environmental policies by defining common standards for 34 spatial

[72] https://www.clinicaltrialsregister.eu/about.html
[73] Appendix, on disclosure rules, to the "Functional specifications for the EU portal and EU database to be audited - EMA/42176/2014", available at: https://www.efpia.eu/media/25185/appendix-to-functional-specifications-of-eu-ct-portal-and-database.pdf
[74] https://www.clinicaltrialsregister.eu/ctr-search/search

data themes (e.g. natural risk zones and energy resources). In times of a crisis such as a forest fire or an eruption of a volcano, having compatible, easily accessible and interoperable data allows governments and local authorities to react more efficiently. Having such data also allows governments and local authorities to predict the impact on their community and to make more informed decisions at the right time. The spatial information is available via an online portal.[75]

[75] https://inspire.ec.europa.eu/about-inspire/563

3.3.12 Rules applicable in the EU research and innovation framework programme

3.3.12.1 Short summary

The Rules for Participation regarding the current 'Horizon 2020' framework programme (2014-2020), established by Regulation (EU) No 1290/2013[76], as well as those proposed for the future 'Horizon Europe' framework programme (2021-2027)[77], include provisions applicable to the data possibly resulting from the projects funded under these programmes.

3.3.12.2 Objectives in relation to data sharing

Without making the sharing of the data mandatory – considering in particular IP rights and the legitimate interests of the beneficiaries of these programmes – the 'Open access' provisions included in their Rules for Participation ('RfP') explicitly encourage such sharing (while open access to publications is mandatory).

- The RfP of the current 'Horizon 2020' framework program state (Art. 43) that:

  "With regard to the dissemination of research data, the grant agreement may, in the context of the open access to and the preservation of research data, lay down terms and conditions under which open access to such results shall be provided, in particular in ERC frontier research and FET (Future and Emerging Technologies) research or in other appropriate areas, and taking into consideration the legitimate interests of the participants and any constraints pertaining to data protection rules, security rules or intellectual property rights. In such cases, the work programme or work plan shall indicate if the dissemination of research data through open access is required."

  More detailed information about the implementation of this provision can be found on pages 246-247 of the Annotated Model Grant Agreement[78].

- The RfP proposed for the future 'Horizon Europe' framework program states (Art. 10) that:

  "Open access to research data shall be ensured in line with the principle 'as open as possible, as closed as necessary'."

3.3.12.3 Parties targeted or affected

The Rules of Participation of the R&I framework programmes apply to all their beneficiaries, i.e. thousands of companies, universities, etc. participating in projects funded under these programmes.

[76] Regulation (EU) No 1290/2013 of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006; see https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/rules_participation/h2020-rules-participation_en.pdf

[77] Proposal available at https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-horizon-europe-regulation_en.pdf

[78] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf#page=246

Considering their large budgets (~70 bn € for Horizon 2020, ~100 bn € for Horizon Europe (proposed)), this means that their provisions affect a large number of entities and of projects.

3.3.12.4 Data targeted or affected

All data generated in the context of projects funded under the R&I framework programmes are concerned. Moreover, such data – in addition to being addressed in the Open Access provisions – are also affected by the general IPR provisions, which govern in particular the ownership of and access rights to data. Indeed, "'results' means any tangible or intangible output of the action, such as data, knowledge or information, that is generated in the action, whatever its form or nature, whether or not it can be protected, as well as any rights attached to it, including intellectual property rights". The access rights provisions are also worth mentioning as they make access to results (including data) mandatory between the participants in a given project (subject to certain conditions).

3.3.12.5 Short assessment of its impact

Although these rules (regarding Open Access and also access rights to the results) only apply, by definition, to the entities participating in projects funded under these framework programmes ('FPs'), they have a significant impact due (1) to the large budgets of the FPs (70 bn € for Horizon 2020), which mean that thousands of research projects and entities are directly affected, and (2) to the role of 'model' that the Rules for Participation of the EU FPs have for the design of other publicly-funded research programmes (e.g. member states' national programmes), meaning that even more entities may be affected, or become affected in the future.

3.4 Non-legislative normative documents with a sector specific focus

3.4.1 Non-legislative normative document: Code of conduct on agricultural data sharing

3.4.1.1 Short summary

It follows from our analysis above that the EU aims to promote data sharing in many contexts. Due to the fact that legislative frameworks are not always capable of providing sufficiently detailed yet flexible, appropriate and commercially reasonable mechanisms of data sharing, alternatives have been sought. An example of such an alternative is the **Code of conduct on agricultural data sharing**.

On April 2018, a coalition of associations from the EU agri-food chain launched a joint EU Code of Conduct on agricultural data sharing by contractual agreement and intends to promote the advantages of sharing agricultural data and enabling agri-business models, including agri-cooperatives and other agri-businesses, to swiftly move into an era of digitally enhanced farming.[79] Compliance with the Code is voluntary.

[79] https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf

3.4.1.2 Objectives in relation to data sharing

The agri-good sector is turning into an era of digitally enhanced farming, where data is generated during all the phases of agricultural production, as well as all related operations. Data has therefore become valuable in the agricultural sector and many experts consider big data to be the next major driver for productivity in agriculture.

Setting up contractual agreements with the purpose of sharing agricultural data is therefore the key component of this Code. The Code promotes the benefits of sharing data and enables agri-business models to move into an era of digitally enhanced farming.

3.4.1.3 Parties targeted or affected

The Code of Conduct applies to the data originator and the party which whom it concludes a contractual arrangement. Everyone could fall within this scope, but given the specificity of the data involved, the parties to this Code will always be entities active in the agricultural sector, such as farmers.

3.4.1.4 Data targeted or affected

According to the Code, agricultural includes, among others, farm data (e.g. agronomic data, compliance data, livestock data), machine data, service data, agri-supply data, and livestock and fish data, land and agronomic data, climate data, machine data, financial data and compliance data. The nature of agricultural data is thus highly specific but very diverse.

3.4.1.5 Short assessment of its impact

The Code contains non-binding guidelines and is not intended to be used as a legal document. However, given that there is no legislation on the topic, it is a major step forward for the agricultural sector.

The Code was launched one year ago, but it has already been accepted and signed by over ten key European agricultural sector organisations, such as the international federations Centre de Liaison International des Marchands de Machines Agricoles et des Reperateurs (CLIMMAR) and AnimalhealthEurope. According to CEJA, the European Council of Young Farmers, all signatories are convinced of the importance of setting transparent principles and guidelines to support the development of digital farming, which demonstrates the need for increased data sharing in agriculture.

4 Summary of the general trends

As the overview of regulatory initiatives above make clear, the principal trend is that there is clearly an **increasing policy interest and regulatory drive** – witnessed by the relatively recent dates of virtually all of these initiatives – to share data. The specific legislative approach to data sharing can take many different forms, depending on the regulatory initiative, including:

- an obligation to make certain data publicly available;
- an obligation to make certain data available upon request (including data porting and data portability provisions);
- an obligation to make certain data available to certain stakeholders;
- an exemption to certain legal protections available to rights holders;
- an obligation to provide information to certain stakeholders that enables or facilitates data sharing.

Nonregulatory interventions which encourage (but do not require) data sharing – notably through Codes of Conduct, as e.g. in the case of data porting under the Free Flow of Non-Personal Data Regulation or the Code of Conduct on Agricultural Data Sharing, but also the focus on open access policies in the PSI Directive – are **increasingly encountered** as well.

Furthermore, data sharing obligations may be constrained or scoped by usage restrictions – e.g. only allowing the recipients of data to use it for specific purposes – or by technical and operational requirements – e.g. the obligation to use certain data formats, or to provide data dynamically through APIs. The latter trend is particularly noticeable: the **emphasis on data sharing services through APIs**, rather than via static data downloads, is a key recurring trend in many newer legislations, including the PSI Directive and PSD 2. This is reflective of the general state of the data economy, which is transitioning to service/cloud-based models in the same way as information society services in general.

In the same vein (i.e. as a further example of legislation following the state of the market), it is remarkable that **research and innovation** are commonly given a priority treatment in legislative initiatives, including in the PSI Directive, the Directive on Copyright in the Digital Single Market (including explicit provisions on text and data mining), and the Database Directive. This can include specific rights, exceptions or carve-outs to ensure that scientific research can be more easily conducted in practice.

Despite these recurring trends, it is worth noting that data sharing provisions can serve many different objectives. Regulatory approaches are shaped largely by the drivers behind the obligation to share data. The principal drivers behind sharing obligations identified in the sections above include:

- facilitating **compliance**, as in the obligation to exchange information on data breaches between data processors and data controllers (with service providers being required to inform their customers on breaches, so that the latter can determine their own legal obligations in case of an incident);

- improving **consumer protection**, as can be seen in the Digital Content Directive's provisions on interoperability, availability and accessibility of digital content;
- enabling fair **competition** and supporting an effective **internal market**, e.g. through the data porting provisions of the Free Flow of Non-Personal Data Regulation; the RMI framework and the Energy Framework;
- encouraging **transparency**, as in the GDPR and ePrivacy Directive's rules on informed consent, notably in relation to traffic and location data sharing; or in the transparency obligations of the Energy Framework;
- supporting **innovation** and **scientific research**, e.g. the exceptions to database rights observed in the Database Directive, allowing extraction for teaching or scientific research; and the comparable provisions on text and data mining in the Directive on Copyright in the Digital Single Market;
- enhancing **security or public safety**, including **public health**, as seen e.g. in the Clinical Trial Regulation, or in the Regulation on road safety-related minimum universal traffic data;
- protecting **fundamental rights**, as seen e.g. in the General Data Protection Regulation and the ePrivacy Directive.

Of course, these drives are archetypes, and very frequently these drivers apply cumulatively: by way of example, the PSD 2 Directive for instance both aims to enable competition and to drive innovation, by ensuring that new entrants in the financial services industry can build competitive services on existing data on equal terms. None the less, the identification of these drivers can help in determining effective implementation policies.

In addition, it is worth underlining that data sharing is not a panacea that represents an optimal policy choice in all circumstances and contexts. Legislation and policy must take into account other considerations, such as economic interests, innovation, competitiveness, and security, all of which can benefit or be harmed by data sharing obligations, depending on scoping and implementation details. For this reason, many regulatory frameworks rightly emphasise such other interests, including the fact that data sharing must be done **securely**, with explicit obligations in relation to implementing **adequate technical and organisational measures** to protect the data. These can be found e.g. in the PSD 2 Directive, but also in the Directive on Copyright in the Digital Single Market.