Report on Data Concepts

There are a number of various terms related to data that are in use in the EU legal and regulatory framework and documentation dealing with data management (including data protection): "personal data", "non-personal data", "public data", "private data", "open data" and other. In expert discussions and in national laws new terms emerge, like "data of general interest". To ensure the consistent application of laws and effective free flow of data, the relationship between the different terms needs to be understood and clear distinction should be drawn.

While many terms may appear synonymous and interchangeable (e.g. "public data" and "open data" or "private data" and "my data"), they have distinct legal meanings that aim to capture various aspects of data management.

Personal data and non-personal data

The distinction between personal and non-personal data is made based on the content of data. **Personal data** is defined in the *General Data Protection Regulation* (GDPR)[1] as "any information relating to an identified or identifiable natural person" (such natural person is called "data subject"). This definition is quite broad, yet precise enough due to further explication that "an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, 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) GDPR).

The test of what is personal data is an objective one (i.e. whether information refers to identified or identifiable person) and does not depend on the circumstances, in which such data has been processed and/ or become available. For example, personal data remains personal data even if it has been published into public domain or obtained in an employment relationship or captured by a private citizen or company.

Personal data – and especially its subset sensitive data[2] – enjoys the highest levels of protection and can be processed only on a limited number of lawful grounds.

The GDPR incentivises pseudonymisation of personal data as it can reduce risks of identification for data subjects. **Pseudonymisation** means the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information" (Article 4 (5) GDPR). In the process of pseudonymisation, certain identifiers are removed that can link data to a person. It is required that such additional information (i.e. identifiers) is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. At the same time, **pseudonymised data remains personal data and the GDPR applies to it in full**.

[1] 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, OJ L 119 of 04.05.2016.

[2] This is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership as well as genetic data, biometric data, data concerning health, sex life or sexual orientation. See Article 9 GDPR "Processing of special categories of personal data".

By contrast, the GDPR does not apply to **anonymous data** (Recital 26 GDPR). Some data is anonymous by its nature, in the sense that it does not relate to an identified or identifiable person (e.g. weather data). Personal data can be rendered anonymous in such a manner that the data subject is not or no longer identifiable: through the process of anonymisation, an anonymised dataset will be created.

There are two main types of **anonymisation techniques**: randomisation and generalisation.[3] **Randomisation** techniques modify the veracity of data. Noise addition renders the attributes less accurate while retaining their overall distribution (e.g. changing the accuracy of dates of birth to ±3 days). Permutation swaps the attributes between different subjects (i.e. breaking the links between the data and data subjects) while exact attributes are retained. Differential privacy is a technique of adding random data (noise) in the original dataset (often while retaining the original dataset and not releasing it to the third party). The difference to the noise addition is that the data controller deliberately decides how much noise to add and in what form and that the original data is not changed, such that the data controller can still identify individuals if necessary.

Generalisation means that attributes of data subjects are generalised by changing the scale or order of magnitude (e.g. from city to country level). Aggregation, K-anonymity, L-diversity, T-closeness are all different techniques of generalisation. The often-mentioned **aggregation** is similar to K-anonymity and means that attribute values of data subject are generalised to such extent that each data subject shares the same values (e.g. dates of birth are grouped by month). This prevents individuals from being singled out from a group where each individual shares the same value within a group of at least K other individuals.

It shall be pointed out that none of the anonymisation techniques guarantees full and complete protection of anonymity, especially in the big data context, and experts recommend using a combination of techniques to render personal data truly anonymous. However, even in this case **de-anonymisation is possible** as a number of experiments have demonstrated.[4] Due to the possibility of de-anonymisation, it may seem like any data could potentially become personal data, which would render the scope of application of the GDPR too broad and all-encompassing.

However, the GDPR provides a **test** to determine whether a natural person is identifiable in situations of pseudonymisation and anonymisation and the data, therefore, is personal. It explains that "account should be taken of all the means reasonably likely to be used" by the data controller or another person to identify the natural person directly or indirectly (Recital 26 GDPR). To examine what means are reasonably likely to be used, one should consider all objective factors, like the costs of and the amount of time required for identification, taking into account the available technology at the time of the processing and technological developments. This effectively means that one and the same data can be considered personal depending on the context (e.g. due to advance in the technology of data analysis, or due to the reduction in cost of data analysis).

The GDPR does not contain any other requirements or criteria for determining whether data is personal data.

---

[3] For detailed description of different techniques, their comparative strengths and weaknesses see Article 29 Data Protection Working Party (2014). Opinion 05/2014 on Anonymisation Techniques, WP216.

[4] See the most recent experiment by MIT urban researchers and planners: http://news.mit.edu/2018/privacy-risks-mobility-data-1207 . This is a known phenomenon (or failure). Similar experiments and studies were conducted as early as 2006. See the famous case of the Netflix Prize dataset: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.3581&rep=rep1&type=pdf .

Non-personal data does not have a definition in law. Rather, it is defined by exclusion: it is "data other than personal data" (Article 1 Regulation on free flow of data). Anonymous and anonymised data, therefore, are non-personal data. The *Regulation on free flow of data*[5] is the main legal instrument governing the circulation of non-personal data. It gives several examples for it: "aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines" (Recital 9 Regulation on free flow of data). Such data can be exchanged and ported without the limitations imposed on personal data.

Public data and private data

The characterisation of data as public or private aims to describe who holds the data in the sense of who is ultimately responsible for and in control of the data.

Concepts different from ownership had to be introduced by law because whether data can be owned is a moot question in legal scholarship.[6] According to the national laws of the absolute majority of EU Member States, data cannot be owned.[7] Even though companies often use the term "ownership" in their contracts that regulate exchange of data, they use it "in a generic and often undefined sense", and it is not clear whether any of such claims will stand in court.[8] It is also worth noticing that, in the data environment, businesses may use the term "owner" with a different connotation, namely not in a legal sense, but as a reference to being responsible for assurance of data quality and curation.[9]

Instead of solving the difficult problem of *personal data* ownership[10], the GDPR established the concept of a data controller that has some obligations similar to an owner. **Data controller** is the person ultimately responsible and accountable for the processing of data: its main distinctive feature is that it determines the purposes and technical and organisational means of processing of personal data (Article 4(7) GDPR). Specifically, the data controller can decide whether to collect personal data, what personal data to collect, for how long, how to modify it - and it has the legal basis for all this. This decision-making power over the data processing means that the data controller is free from instructions of others and that it is responsible for lawfulness and accuracy of data processing. Data controller can be a natural or legal person, public authority, agency or other body. It exercises the control over and responsibility of the data processing either alone or jointly with another entity (i.e. joint controllers).

Data controller can process the data itself or outsource this task completely or partially to a different entity called "data processor" in the GDPR. The main defining feature of a **data processor** is that it is

[5] Regulation (EU) 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, OJ L 303 of 28.11.2018.
[6] In the light of the importance data play is the economy, there are studies that call for a new ownership right. See, for example, the While Paper on Data Ownership drafted in the course of the TOREADOR project: https://www.twobirds.com/en/news/articles/2017/global/data-ownership-in-the-context-of-the-european-data-economy
[7] See Deloitte et al. (2018). Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability - SMART 2016/0030, Annex 1.
[8] Deloitte et al. (2018). Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability - SMART 2016/0030, pp. 73-75.
[9] OECD (2015). Data-driven Innovation: Big Data for Growth and Wellbeing, p. 195.
[10] Arguably, the question of data ownership cannot be solved by an EU regulation due to the lack of competences of the EU to intervene and change the property ownership laws of its Member States. See Article 345 TFEU: "The Treaties shall in no way prejudice the rules in Member States governing the system of property ownership."

processing data on behalf of the data controller (Article 4(8) GDPR). "Processing" means any operation or set of operations performed on personal data, "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) GDPR). To be considered a data processor, an entity needs to stay within the limits of the task imposed by the data controller. If the data processor starts merging data received upon delegation with its own databases or starts using it for its own purposes, not agreed with the data controller, then such data processor becomes a (joint) data controller.

In case of *non-personal data*, unfortunately, the legislators used terminology that is different from the GDPR. The Regulation on free flow of data also uses the term "**service provider**" for a natural or legal person providing data processing services. Data processing defined by the Regulation in the same way as in the GDPR (Article 3(2) Regulation). This seems to suggest that the term "service provider" in the case of non-personal data signifies the same as the term "data processor" in the case of personal data.

However, it is not entirely clear who can be considered the data controller in the case of non-personal data. The Regulation on free flow of data contains the term "**user**" that means a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service (Article 3(7)). It also uses the term "**professional user**" for those who uses or requests a data processing service for purposes related to its trade, business, craft, profession or task (Article 3(8)). The definitions of both terms lack the clear attribution of control and ultimately responsible for the data. However, from the recitals of the Regulation it is sufficiently clear that users are the ones with the decision-making power over "their" data because they choose service providers, request various data processing services from them and can port data from provider to provider.

In this submission, for purposes of conciseness, the terms "publicly held data" and "privately held data" will be used depending on who is ultimately in control of the data, both personal and non-personal. In the former case, it is a public authority or other public body. In the latter case, it is an individual or legal person of civil law.

For **publicly held data**, the main document at the EU level regulating the flow of such data is Directive 2003/98/EC on the re-use of public sector information (*PSI Directive*). This Directive is under revision and will be soon replaced by the new *Open Data and Public Sector Information Directive*[11]. The new Directive will significantly expand the scope of its application and cover not only data that are held by public sector bodies, but also data produced in the performance of services in the general interest by public undertakings (e.g. in the utilities and transport sectors) and to research data resulting from publicly-funded research or co-funded by public and private entities.

It shall be noted that the new Open Data and Public Sector Information Directive uses the terms "public data", "public sector information", "datasets" and "documents" interchangeably across its

[11] The political agreement between the European Parliament, the Council and the European Commission was reached on 22 January 2019: https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive .

text.[12] This may lead to some difficulties in the implementation because all four terms have distinctly different meaning in their conventional use and also when used in other legal documents.

The most relevant legal instruments that could be protecting **privately held data** are those dealing with various intellectual property rights: Trade Secrets Directive[13], Database Directive[14] and Information Society Directive[15].

The *Trade Secrets Directive* protects any data and information in possession of an undertaking as long as these data:

a) is secret (not generally known among or readily accessible to persons within the relevant circles of trade),
b) has commercial value because it is secret, and
c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

This means that, potentially, the Trade Secret Directive could be used to protect raw data and other data – as long as they are kept secret.

The *Database Directive* grants copyright protection only to collections of data which are arranged in a systematic or methodical way and are individually accessible by electronic or other means. To claim the copyright protection, a database needs to constitute author's intellectual creation, meaning that it needs to be original. At the same time, it shall be noted that the specific object of protection is the database structure, not the individual elements contained in the database. In fact, databases are often created with elements/ data that are in the public domain.

The Database Directive also grants the so-called sui generis protection to databases. This type of protection rewards the qualitative and/or quantitative substantial investment in creating the database (i.e. 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). Any substantial change to the contents of the database, that could be considered to be a new investment, will renew the term of the sui generis protection. In the context of big data collection, which is extremely dynamic, may result in unlimited sui generis protection of databases.

The *InfoSoc Directive* can provide copyright protection to data if two requirements are met:

1) The data in question is fixed in a tangible form (e.g. electronic archives or digital files – as long as it remains concrete, can be easily identified and described) and
2) The data is original meaning it should possess a level of sophistication, the threshold of which is relatively low in most EU Member States.[16]

[12] The Directive uses terms "data", "information" and "documents" interchangeably. It gives definition only to "documents": "any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording)" (Article 2(5)).
[13] Directive (EU) 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, OJ L 157 of 15.6.2016.
[14] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77 of 27.3.1996.
[15] 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, OJ L 167 of 22.6.2001.
[16] While Paper on Data Ownership, p. 69.

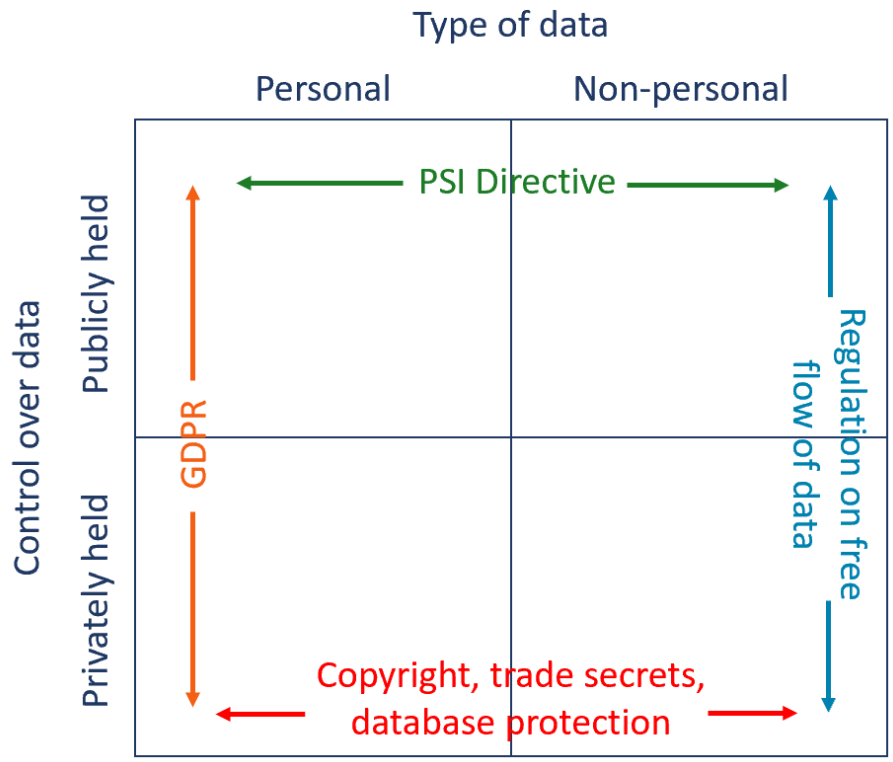
Due to these requirements, not all data can be protected by copyright. For example, processed data presented in a graphic form is more likely to enjoy copyright protection than raw data, measurements from sensors, data from automated processes and metadata.

Taxonomy of data concepts

The juxtaposition of the data concepts related to the types of data and data-holders results in the following scheme (see Figure 1 below). The figure describes the relation between the types of data and data-holding. It also shows what main legal instruments are applicable to protection and movement of data at the EU level. Other legal instruments that may be applicable to different types of data are not depicted for the sake of conciseness.

Considering the extension of the application scope of the new Open Data and PSI Directive to include data produced in the performance of services in the general interest by public undertakings and research data resulting from publicly-funded research or co-funded by public and private entities, such data will fall under the publicly held data. Data produced by such undertakings in other circumstances is likely to be classified as privately held.

Figure 1 Taxonomy of data concepts



Data of general interest

The notion of "data of general interest" has been introduced in the French Digital Agenda of 2015. It was said there that data of general interest refers to data from public and private actors, whose opening presents a strong stake of general interest. Following this, a study into the notion has been launched in preparation to the Digital Republic Law.[17] It should be noted that the study did not produce a definition of "data of general interest", and it used this term interchangeably with the

[17] See the full report: https://www.economie.gouv.fr/republique-numerique-ouverture-donnees-d-interet-general .

term “essential data”. It seems that one of the aims of the study was to research legal opportunities for public authorities to extract data held by private companies.

The study directly linked the notions of “essential data” and “data of general interest” to the activities of the so-called SPIC undertakings (i.e. undertakings providing “service public à caractère industriel et commercial”). It recommended that data on public concession contracts and their execution, on public subsidies/ grants and their use and essential data generated by SPIC undertakings should be published in open access. The study suggests introducing, by default, open data clauses concerning the exploitation of data in public concession contracts.

On the basis of the study, several articles related to “data of general interest” were included in the *Digital Republic Law*[18]:

1) When a public authority delegates public service obligations (e.g. waste management) to an undertaking, it may contractually require the undertaking to provide to the authority the detailed data collected while carrying out the public service.
2) For grants of over EUR 23.000 awarded to undertakings, the public authority is required to publish essential information, such as the name of the beneficiary, the amount of grant, the object and duration of the agreement.
3) Legal persons can be required to transmit data held in their databases directly to the National Institute for Statistics and Economic Studies (INSEE) – exclusively for purposes of statistical studies.
4) Managers of public roads and by managers of the public distribution and transmission networks for electricity and for natural gas are required to make certain data (e.g. on consumption and production) available for re-use.

The approach and the suggestions developed in the French study have found their way into the EU legislation. As mentioned above, the new *Open Data and Public Sector Information Directive* will be applicable to documents held by public undertakings entrusted with services of general interest, public service operators and other public undertakings fulfilling public service obligations (Article 1(1)b). All documents produced by such public undertakings in the scope of the provision of services in the general interest shall be re-usable for commercial or non-commercial purposes (Article 3).

The scope of application of the French law seems to be much broader than the said new Directive because it applies to all undertakings entrusted with services of general interest, while the future EU Directive will apply only to public undertakings. “Public undertaking” is defined as undertaking over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it (Article 2).

Central for the understanding of the concept of data of general interest is the **understanding of the general interest**. What exactly is it? The notion of general interest is widely used in the EU law in connection with services, and the Member States have the competence to define which services they consider to be of general interest. The provision of such services is subject to a special legal regime that is usually different from the competitive provision by the market. Usually, a public or private undertaking receives a concession and/or obligation to provide services of general interest under specified conditions.

[18] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique: https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/texte#JORFSCTA000033202839 /

The EU law distinguished between services of general economic interest (e.g. telecommunications, post), non-economic services (e.g. justice and policing) and social services of general interest (e.g. social security, social housing). However, the EU law does not define the general interest – because this is left to Member States. The designation of general interest varies from state to state as it depends on national legal traditions and on the dynamics of the economic and social development. What is considered general interest is a political decision by an individual state and, therefore, varies strongly from state to state. Accordingly, the service provided in general interest, their exact contents vary from state to state, too. It is therefore likely that, if the notion of general interest would apply to data, different types of data will be covered.

The definition of general interest may range from the core tasks of public authorities (i.e. public safety, public security, public health) to a very broad one covering all areas of societal activity. Examples of the former approach can be found in almost all legal instruments on data management. The *Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications* refers to the classical set of special interests, including "including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (Recital 26).[19] It is typical that data related to these narrowly defined public interest areas has to be made available to the competent authorities upon their request. An example of the broad approach can be found in the French study. It developed four categories of general interest[20]: 1) optimisation of sectoral public policies, 2) better information for citizens, 3) contribution to scientific research and 4) economic development.

Whatever the general interest is exactly, it cannot cover the whole amount of data. Yet, it may cover different types of data (i.e. personal and non-personal). The data that is of general interest may happen to be held by a private or public entity. Figure 2 below shows what the data taxonomy looks like if data of general interest is introduced.

[19] 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, COM(2017) 10 of 10.01.2017.
[20] Report, p. 45.

Figure 2 Taxonomy of data including data of general interest

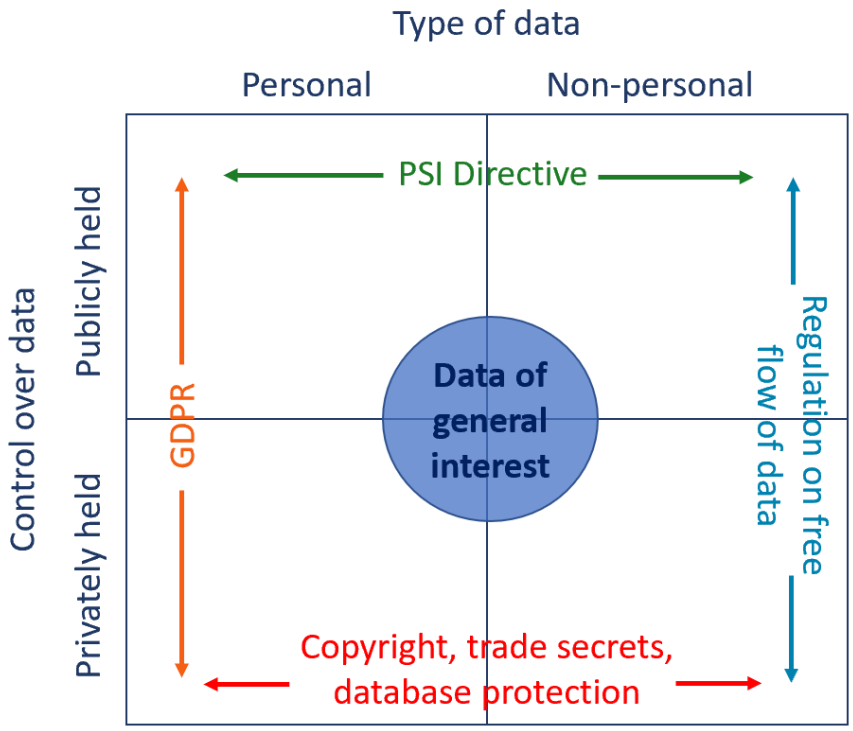


Figure 2 also illustrates that, depending on the type and data holding, a **different set of rules will be applicable to re-use and sharing of such data**. For instance, if personal data may be of general interest (in the context of public safety or public health), one would need to consider the GDPR implications. In addition, if such personal data is privately held in a database (e.g. data of medical research or test), then database protection rules may be additionally applicable. This means that, depending on the data, different mechanisms need to be developed and employed to make the data available for re-use while, at the same time, ensuring the rights of data-holders and data subjects.

The European Commission has developed a *Guidance on sharing private sector data*[21], which provides a toolbox for data holders and data users. The document contains principles for business-to-government and business-to-business data sharing as well as models of data sharing and related legal and practical considerations.

A separate question to consider is whether all data of general interest is also open data.

Open data

The concept of open data refers to the mode of access to and use of data. Open data is data that anyone can access, use and share. Data can be in open access disregarding whether it is publicly held or privately held. At the same time, even publicly held data can be closed to public access for the reasons of public security and safety.

[21] Commission Staff Working Document. Guidance on sharing private sector data in the European data economy. SWD(2018) 125 final of 25.04.2018.

A number of studies, including empirical studies, advocate and document benefits of open data.[22] This is the reason why the EU is promoting access to data across. The PSI Directive is the main legal instrument encouraging open access to publicly held data by public authorities and other public bodies of Member States. Member States have been adopting relevant laws and creating open data portals at national, regional and municipal levels.[23] These national portals are often called Open Government Data.

At the EU level, the EU institutions aim to make their data publicly available whenever possible; it is also free of charge for all users and has no copyright restrictions on it. At the EU level, the main document governing this data and the process of making it available refers only to the data of the European Commission, namely *European Commission Decision 2011/833/EU on the reuse of Commission documents*.[24] This document is not binding on any other EU institutions.

In terms of data taxonomy, all non-personal data that is held by the European Commission (top right box) is likely to be in open access. The small exception would be various types of confidential data, data/ documents that are covered by various intellectual property rights (patens, copyright, trademarks etc) for which the Commission is not in a position to authorise access and data/ document from ongoing research (Article 2(2) Commission Decision). All open data is published on the EU Open Data Portal.[25]

As mentioned above, open data signified the legal regime of access to such data which is open to the general public. This submission argues that depending on the type of data, its origins (public v private), other rights related to it and on the nature of the general interest attached, the legislator may need to consider **different legal regimes of access to data of general interest**. While the French Digital Republic Law provided open access to many categories of data of general interest (i.e. made it open data), the current EU legislation on data protection and on free flow of data contains some indications to this end.

The first case is the data that may be in general interest (e.g. crime prevention or public health), but that is also personal data. Such data can be publicly held or it can requested from private entities, that happen to hold it, by competent authorities. However, such data cannot be released into open access under the GDPR.

The second case is non-personal data that is of general interest and that is clearly public sector information, but should be subject for a more restricted access. For example, it may appear reasonable to restrict public access to certain data related to public health or security in order to prevent panic and not to disrupt the public order.

[22] See a short summary in Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer (2017). The economics of ownership, access and trade in digital data; Digital Economy Working Paper 2017-01; JRC Technical Reports, p. 42.

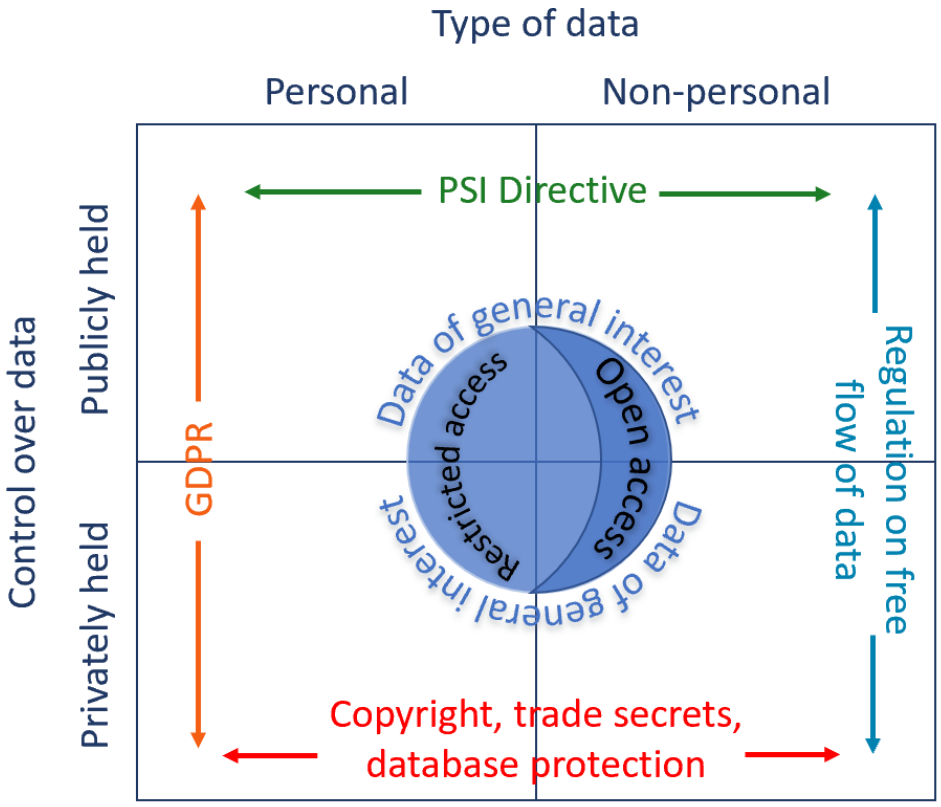
[23] For example, in Germany, the open data provision is regulated by the so called E-Government Law od 2017 (Gesetz zur Förderung der elektronischen Verwaltung, can be found here: http://www.gesetze-im-internet.de/egovg/ . Several different open data portals were created, namely https://www.govdata.de/ for the national level, https://open.nrw/ for the regional level of North Rhine-Westphalia, but there aer respective portals for each region, and https://oknrw.de/ for the municipal level of North Rhine-Westphalia.

[24] OJ L 330 of 14.12.2011.

[25] https://data.europa.eu/euodp/en/home .

The third case is non-personal data that is privately held and is of general interest. However, if this data also commercially sensitive or subject to copyright, the private holder may refuse its release to the general public and restrict the access to the public authority alone.

Figure 3 Data taxonomy, including data of general interest and mode of access



The *INSPIRE Directive*[26] contains a list of public interest reasons that can justify the limitation of public access to spatial data. It stipulates that the reasons for the limitation of access should be interpreted narrowly and suggests that, in every particular case, "the public interest served by disclosure shall be weighed against the interest served by limiting or conditioning the access" (Article 13 para. 2). The same provision is contained in the *Directive on public access to environmental information* (Article 4 para. 2)[27].

Between open data and closed data (which could be considered as extreme cases of data access and use), there are many options of restricted access to data.[28] Where a government requests the release of privately held data into open access, special contractual arrangements may be necessary in order to ensure the relevant rights, obligations and interest of the private holder. These include not only its obligations under the GDPR, rights stemming from copyright, but also economic interests linked to raw data collection, data processing and maintenance. The Commission's *Guidance on*

[26] 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, OJ L 108 of 25.4.2007.
[27] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, OJ L 41 of 14.2.2003.
[28] For analysis of closed and open data systems see Clare Birchall (2016). Shareveillance: Subjectivity between open and closed data, in: Big Data & Society, pp. 1–12, available at: https://journals.sagepub.com/doi/pdf/10.1177/2053951716663965 .

sharing private sector data contains recommendations on the B2G models of data sharing that will come in handy also for data of general interest.

Author: Olga Batura

Email: Olga.Batura@ecorys.com