Data and licensing management guidelines

Research report and guidelines prepared within the project

STIRData: Specifications and Tools for Interoperable and Reusable data

co-financed by the Connecting Europe Facility Programme of the European Union, under GA n. INEA/CEF/ICT/A2019/2063078

Author: Jakub Míšek, Ph.D., Radim Charvát, Ph.D., Matěj Myška, Ph.D.

Masaryk University, Faculty of Law

November 2022

This research report and guidelines were prepared within the project “STIRData: Specifications and Tools for Interoperable and Reusable data” co-financed by the Connecting Europe Facility Programme of the European Union, under GA n. INEA/CEF/ICT/A2019/2063078.

The availability of resources has been verified as of 31 October 2022, unless a different date is specified for a particular resource.

1. Introduction and methodology

Open data is a global phenomenon that aims to enable the effective use of public sector information (PSI).[1] When we are discussing PSI and its legal regulation, we firstly need to divide two basic layers – access to PSI and its re-use. Public administrations and local governments produce large amounts of information and data in the course of their statutory tasks. Whether it is, for example, the files on the basis of which the law is applied authoritatively, the environmental data used to decide whether or not to allow construction, or, if we look a level higher, the data used to determine policies for the future development of the state or parts of it, it is always data that the public administration works with and on the basis of which it produces any of its outputs. Being able to see the data that has led to such outputs, or even the outputs themselves, is then a prerequisite for effective scrutiny of the performance of public administration by civil society. Furthermore, right to access the data (or PSI in general) is a necessary part of freedom of speech, a basic political right that allows for transparency and public scrutiny of how public sector bodies fulfil their duties. Without access to specific important data, it would not be possible to hold a public discussion regarding the actions of our elected officials and public sector bodies.[2]

In addition to the above, there is high value potential in public sector data, best characterised by the statement of Rufus Pollock, founder of the Open Knowledge Foundation, who argued that "*The best thing to do with your data will be thought of by someone else*". This aspect of public sector data relates to the possibility of its subsequent and repeated use. The economic value of public sector data lies, for example, in enabling financial savings by linking data that would otherwise be separated due to their different originators,[3] or in developing applications that offer better services to citizens who are happy to pay for them,[4] thereby creating a market that generates economic benefits as indicated by profitability, tax collection, employment and other factors. In its study, the McKinsey Global Institute analysed seven areas (education, transport, consumer products, energy, oil and gas, healthcare and consumer finance) and quantified the potential value inherent in the effective publication and re-use of data in these areas at over USD 3 000 billion per

[1] Parts of this analysis draw upon *inter alia* the results of previous research of the main author, which was concluded by a rigorous thesis defended in 2019 (MÍŠEK, Jakub. *Právní aspekty otevřených dat* [online]. Brno, 2019. Online in Czech: https://is.muni.cz/th/sqe7a/. Rigorous thesis. Masaryk University, Faculty of Law.).

[2] A good example of such a situation was a very difficult access to health data relating to the COVID-19 pandemic in the Czech Republic, which then further led to a diminishing of public trust.

[3] E.g. Jetzek Thorhildur, Michel Avital and Niels Bjørn-Andersen, 'Generating Value from Open Government Data', *International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design* (2013) 16.

[4] E.g. Melissa Lee, Esteve Almirall and Jonathan Wareham, 'Open Data and Civic Apps: First-Generation Failures, Second-Generation Improvements' (2016) 59 Communications of the ACM 82, 89.

year.[5] The growing potential of public sector data has also been recognised by the European Union, which since the beginning of the new millennium has been involved through its legislation in promoting the usability of public sector data in its Member States.[6] In addition to the economic benefits, however, we can also talk about the 'societal value' of such data, for example in terms of greater citizen engagement in public affairs in the form of policy planning affecting economic growth, education, conservation, security and other areas of public life. [7]

Access to PSI and its re-use are two interrelated phenomena, where the latter cannot naturally occur without the former. However, different legal regimes apply to the two. In the case of PSI access, it is primarily a public authority activity. This is even though this activity is often initiated by a person who has a fundamental right to information and who therefore has the right to demand positive performance from the state in the form of providing it. The provision or non-provision of PSI is then a direct exercise of public authority in the field of information rights, with all the consequences that this entails.

In contrast, the re-use of PSI primarily concerns the recipients of the data, i.e. third parties who further handle the data. In this case, the law regulates how they can dispose of the data, how they are limited in this disposal and what obligations they have to fulfil. The basic principle that applies in this case is the principle of legal licence, according to which anyone can do what is not prohibited by law. However, the mere fact that the applicant has the right to access the data does not in itself mean that they can use freely all the data thus obtained. On the contrary, they are still limited by protective institutes such as personal data protection, intellectual property rights and others. Furthermore, a large part of the regulation of PSI re-use is legislation that ensures that data providers provide data in a way that makes it as easy as possible to use. Making the data available in appropriate formats and under clearly defined legal conditions is a prerequisite for enabling its subsequent re-use.

The concept of public sector data re-use has recently been closely linked to the concept of open data as a technologically efficient way of providing and re-using PSI. Of course, one of the possible

---

[5] MCKINSEY GLOBAL INSTITUTE. Open data: Unlocking innovation and performance with liquid information | McKinsey & Company [online]. 2013 [seen 31. 10. 2022]. Online: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.

[6] See Directive 2003/98/EC, its amendment Directive 2013/37/EU and then the newest recast, Directive EU No. 2019/1024.

[7] See e.g. Erna Ruijer and Evelijn Martinius, 'Researching the Democratic Impact of Open Government Data: A Systematic Literature Review' (2017) 22 Information Polity: The International Journal of Government & Democracy in the Information Age 233; Igbal Safarov, Albert Meijer and Stephan Grimmelikhuijsen, 'Utilization of Open Government Data: A Systematic Literature Review of Types, Conditions, Effects and Users' (2017) 22 Information Polity: The International Journal of Government & Democracy in the Information Age 1.

uses of such data is in public control. However, this is not an automatic consequence of the provision and use of PSI. In recent years there has been an inappropriate conflation of the terms open data and 'open government', in the sense of transparent and auditable public administration.[8] However, open data in itself has no value in the pursuit of open government. Governance can be transparent without the efficiencies brought by new technologies. Equally, public authorities may provide a lot of open data, but it will not contribute in any way to greater transparency in the exercise of public authority (e.g. public transport timetables).[9] It always depends very much on the specific nature of the data provided, i.e. what it tells us. This is also why, in the context of political right, which is used to control public administration, it is mainly access to PSI on the basis of requests. As Peixoto goes on to argue, even if data is by its nature capable of providing better control of public administration, other factors such as a free media and a mature political culture are necessary for the actual exercise of such control.[10]

It is necessary to stress out, that at least from the legal perspective, open data are understood as highly efficient way of providing PSI for the easiest further re-use. When we are discussing open data and its legal regulation, we are answering mostly the question “how” is PSI provided. The question “what” PSI is provided is subjected to specific regimes of access to PSI. However, when deciding on the question what data a public sector body can publish and how it should be done, both of these layers must be analysed and tackled.

This analysis focuses on the legal issues of open data publication and re-use, with a focus on the datasets of public registers of companies and other legal entities, as this is the main research goal of the whole STIRData project. Nevertheless, the conclusions and recommendations arising from this legal analysis are applicable in broader scope of any PSI and open data publication and re-use.

The aim of this analysis is firstly to provide a guidance for open data providers on what are the relevant legal questions during the publication process. Secondly, this document should help the open data providers find answers, or at least point them to the sources of the answers in their respective legal orders, on these relevant questions. Thirdly, for the sake of completeness, where relevant, this document aims to provide at least a basic overview of relevant legal questions regarding the re-use of open data. Therefore, this document is divided into two main parts: I) Legal

[8] Some authors, such as Evgeny Morozov, then criticize the consequences of such merging of originally technical and social concepts, as they blur the boundaries between them, giving rise to the illusion that many problems can be solved "*at the click of a button*". See Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (PublicAffairs 2013) Chapter 3.

[9] Harlan Yu and David G Robinson, ‘The New Ambiguity of Open Government’ (2011) 59 UCLA Law Review Discourse 178.

[10] Tiago Peixoto, ‘The Uncertain Relationship between Open Data and Accountability: A Response to Yu and Robinson’s the New Ambiguity of Open Government’ [2012] UCLA Law Review Discourse 200.

analysis and II) Guidelines and a licencing scheme. The first part provides theoretical and argumentation background for the second part, which is more practically oriented. It offers a checklist of steps, which must be considered during publication of open data in order to ensure that the data are provided legally and in the most reusable way.

The first part is divided into four chapters (Chapters 2 to 5). Chapter 2 offers a brief overview of relevant international and European Union legal instruments that regulate access and re-use of PSI, both existing and anticipated. It also puts into context the position of datasets of public registers of companies and other legal entities. Chapter 3 focuses on the issues of intellectual property protection, which can pose in certain situations an obstacle for publication and re-use of PSI and open data especially. The chapter, from the perspective of international and European Union law, briefly explains basic concepts of copyright and database protection. It also provides a recommendation on licensing schemes and use of public licences. Chapter 4 focuses on the questions of personal data protection, because this issue is very deeply connected with the publication and re-use of datasets of public registers of companies and other legal entities, as they contain a lot of personal data regarding ownership of companies. Finally, chapter 5 offers recommendations on how to properly prepare terms of use and what licences to use in which cases.

This analysis is prepared from the perspective of international and European Union law. That is because a preparation of detailed analysis that would incorporate specifics of member states is out of the scope of the STIRData project. The focus on the international and European Union law represents the main limitation of this analysis. However, at the same time, it ensures its flexibility and applicability regardless the specific national jurisdiction, because the international and European Union legal instruments offer a common harmonised framework which is applicable throughout the EU.

Part I: Legal analysis

2. International and EU law

2.1 International treaties

On the level of international treaties, the focus is on access to PSI and not its re-use. Furthermore, even the access to PSI was historically hidden as a part of freedom of expression, rather than an independent right. The right to information first became relevant in the 1948 Universal Declaration of Human Rights, Article 19 of which declares the right to freedom of expression, including the right to seek, receive and impart information and ideas by any means.[11] Next, and probably the most important one of them, was European Convention on Human Rights (1950), Art. 10 para. 1 of which ensures freedom of expression as follows: "*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*" Again, we can see that access to information is inherently part of freedom of expression. This legal construct was confirmed also by the European Court of Human Rights in the case Magyar Helsinki Bizottság v. Hungary.[12]

The Convention allows for limitation of freedom of expression, and accordingly, right to access the information. It states that "*[t]he exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*."[13] Furthermore, we can find the same construction in the International Covenant on Civil and Political Rights (1966).[14]

From the point of view of the historical development of the right to information, other documents of the Council of Europe are interesting, even if they are only of a recommendatory nature.[15] They

---

[11] Art. 19 reads as follows: "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*"

[12] Decision of the Grand Chamber of European Court of Human Rights from 8. 11. 2016, No. 18030/11 (Magyar Helsinki Bizottság v. Hungary).

[13] Art. 10 para. 2 European Convention on Human Rights.

[14] Art. 19 of International Covenant on Civil and Political Rights.

[15] E.g. Declaration of the Committee of Ministers of the Council of Europe on Freedom of Expression of Information of 29 April 1982.

contain basic principles that are still a key part of the right to information. They are as follows: i) Every person has the right to receive information held by public authorities; ii) The applicant for information is not obliged to prove the reasons for his/her request; iii) Access to information is to be exercised on the basis of the principle of equality; iv) Information is to be provided within a reasonable time; v) State authority must state the reasons for withholding information; and vi) Rejection of a request must be reviewable.

More recently, the Council of Europe has prepared a Convention on Access to Official Documents (CETS No 205; Tromsø, 18 June 2009), which aims to create "*genuine starting point for an effective right of access to official documents in the European region*".[16] Convention No 205 guarantees the right of any person to have access on request to official documents (PSI) held by public authorities. These are defined quite broadly in the Convention and include, in addition to state and local authorities, legislative bodies, the judiciary and natural and legal persons when they exercise public powers. However, this is only the minimum necessary set of entities - ratifying States may decide on a broader definition of obliged entity. The Convention regulates possible restrictions on the provision of information and generally addresses the proceeding of making a request, including its processing. In terms of re-use of information, Convention 205 does not offer specific regulation.[17] Currently, 10 Council of Europe countries have ratified Convention 205, including Finland, Estonia, Lithuania, Hungary and Montenegro.

2.2 Law of European Union

The right of access to information, or the obligation of public authorities to provide certain information, has not received much attention in the context of European law. The fundamental provision of European law dealing with the right of access to information is the Charter of Fundamental Rights and Freedoms of the European Union.[18] It includes the right to information as part of the right to freedom of expression under Article 11, but it also includes, in Article 42, a specific right of access to documents of the Union's institutions, bodies and other entities, irrespective of the medium in which the documents are held. At the level of secondary legislation, this right is expressed in general terms in relation to the institutions of the European Union by Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

---

[16] See the Explanatory Report to the Convention [online, cit. 25. 7. 2021]. http://www.worldlii.org/int/other/COETSER/2009/2.html

[17] See Mireille Van Eechoud and Katleen Janssen, 'Rights of Access to Public Sector Information' (2013) 6 Masaryk University Journal of Law and Technology 471.

[18] Document No. 2010/C83/02.

Although European legislation is not very rich in the field of legal regulation of access to information,[19] the situation is quite different in the field of legal regulation of the re-use of PSI. In fact, the European Union (or formerly the European Community) has been the main driving force in the European area in the field of introducing legislation enabling the re-use of PSI since the 1980s.[20] In 1989 the Commission issued "*Guidelines for improving the synergy between the public and the private sectors in the information market*".[21] Article 1 stated that public organisations should make their information available to the private sector in a reusable form through electronic information services. Exceptions could be made in cases where access to information was precluded on grounds of legitimate public interest. However, binding legislation at secondary law level only came with Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, popularly known as the 'PSI Directive'. The primary objective of PSI Directive was to create a workable legal environment for the transparent and non-discriminatory use of public sector information published for this purpose. It should be stressed that the PSI Directive did not impose any obligation to provide information. It merely stipulated that, where information is provided, it should be done in such a way as to facilitate as far as possible its re-use by the private sector. This approach has not been changed by its amendment in the form of Directive 2013/37/EU nor later.

Directive 2003/98/EC, as amended by Directive 2013/37/EC, set out at a general level the basic rules and principles aimed at the re-usability of published public sector information. The Directive was applied to all documents[22] made available by public sector bodies, except where specified in the Directive. These included documents that do not fall within the scope of the public tasks of the public sector body concerned, documents encumbered by third party intellectual property rights, documents with restricted access for reasons of data protection and documents held by cultural institutions other than libraries, museums and archives.[23] Thus, a there may have been a situation where national law allowed for the provision of a document (i.e. access to it), but since the document was covered by an exception to the application of the Directive, the State concerned

[19] It must be noted that there is a problematic and yet unresolved issue whether the European Union even has the competence to oblige Member States to ensure general access to public sector information. See Eechoud and Janssen (n 16) 478–480.

[20] For more context see Herbert Burkert, 'Public Sector Information: Towards a More Comprehensive Approach in Information Law' [1992] Journal of Law and Information Science 47, 49.

[21] Online: https://op.europa.eu/en/publication-detail/-/publication/7c37bbee-4363-4ec7-91ff-b6848142ec97/language-en

[22] The term document is broadly defined in Art. 2 para. 3 as "*any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording)*" or any part of such content.

[23] The exemption from the exception, i.e. the return of libraries, museums and archives to the scope of application of the Directive, is a novelty introduced by Directive 2013/37/EU. Its importance is seen particularly in the context of facilitating the digitisation and dissemination of the content of library collections.

was not obliged to ensure the re-usability of such information.[24] The general principle of the Directive was to ensure that information is provided as openly as possible (both technically and legally) so that it is as easily reusable as possible.

It is important to note that the directive does not differentiate a situation when the data is provided voluntarily on the discretion of data provide and a situation when there is an existing legal duty to provide the data (regardless of whether it arises from the EU or national law). In both cases, voluntary and mandatory data provision, the principles of the directive and duties arising from it will apply, because it is assumed that even voluntary data publication is done in accordance with the law of the member state. Thus, if it falls within the scope of the directive, the directive will apply.[25] However, data provider should be aware of their national legal duties and should check whether they have to or at least can provide data in question.

PSI directive was replaced by directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information (further "OD Directive"), which preserves the same grounding principles as the previous legal instrument. OD Directive, which is a recast of the PSI directive, became applicable on 17 July 2021.

Art. 1 para. 2 OD Directive sets a list of exceptions, which are out of scope of the directive. In the context of this analysis the most important are:

- "*c) documents for which third parties hold intellectual property rights*
- *d) documents, such as sensitive data, which are excluded from access by virtue of the access regimes in the Member State, including on grounds of:*
    - *the protection of national security (namely, State security), defence, or public security;*
    - *statistical confidentiality;*
    - *commercial confidentiality (including business, professional or company secrets);*
- *h) documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of*

[24] As an example we can mention copyrighted work of a third party which the public sector body provides for access, but cannot licence for further re-use.
[25] E.g. in the Czech Republic quite a lot of databases and information sources are provided mandatorily on the legal bases, however there also exists a possibility of a voluntary data publication, because of a general discretion to do so given by the section 5 para. 5 of the Freedom of Information Act (act No. 106/1999 Sb.).

the individual, in particular in accordance with Union or national law regarding the protection of personal data".

It is important to realise, that letter h) does not exempt from the application of OD Directive personal data processing altogether. If European or national law allows for or demands publication of datasets containing personal data, the OD Directive will generally apply, unless there is another kind of exception on the level of national law.

The general principle of the directive is formulated in Art 3 para. 1 as follows: "[…] *Member States shall ensure that documents to which this Directive applies in accordance with Article 1 shall be re-usable for commercial or non-commercial purposes … .*"[26] Art. 5 para. 1 sets basic requirements for the quality of provided documents. They must be made available in "*any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open,*[27] *machine-readable,*[28] *accessible, findable and re-usable, together with their metadata*". Furthermore, both format and metadata should, where possible, be compliant with "*formal open standards*".[29] Formal open standard is defined as a "*standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability*"[30] and it is an important, albeit sometimes overlooked, tool for ensuring interoperability of content provided by different providers. When the same type of dataset is provided by multiple data providers in their specific fields, it can easily lead to a multiplicity of data standards, which would lower the possibility of effective connection and re-use of such data. European legislator realised the necessity for interoperability, however at the same time, it is not possible to legislate specific technical standards at this legislative level. Therefore, the concept of formal open standards was introduced. A formal open standard means a non-legislated technical normative document that describes in a great detail how (in what formats and structures) the data is to be provided. The OD Directive does not provide for any official authority to issue formal open standards. The advantage of a formal open standard is its flexibility. As it may become necessary to specify formal open standards in more detail or update them in the course of their use and lifetime in the light of technical developments, the informal way in which they are issued is an appropriate feature. At

[26] As in the previous directive, the term "document" means any content whatever its medium or any of its parts.
[27] Open format is defined in Art. 2 para. 14 as "*a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents*".
[28] Machine-readable format is defined in Art. 2 para. 13 as "*a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure".*
[29] Art. 5 para. 1 OD Directive.
[30] Art. 2 para. 15 OD Directive.

the same time, a formal open standard is a purely technical document, whose primary audience is the people who directly prepare the data for publication (usually the IT department).

The OD Directive also covers the question of costs for provided information and data. Art. 6 stipulates the general rule that the re-use of documents must be free of charge. As a general exception from this rule, the data providers can demand "*the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information*", which includes also costs for particularly extensive search for requested information.[31] Art. 6 para. 2 enumerates specific exceptions from the general rule of costless access to and re-use of PSI, however none of those are relevant for the scope of this report.

OD Directive is built on PSI Directive, but it also brought several new important concepts. It has broadened the scope of its application to public undertakings[32] and research data,[33] it introduced rules for providing dynamic data[34] and it in fact excluded application of sui generis database right protection,[35] to name a few. In the context of this analysis probably the most important change is the introduction of so called "*High Value Datasets*" (further HVDs). The idea of the legislator behind this concept was that certain types of data are so important Union-wide for their socio-economic potential, that they should be mandatorily provided by each member state.[36] Therefore, based on Art. 13 OD Directive was created the Annex I of the directive, which a list of general categories of important data. Specific datasets, which will be mandatorily provided EU-wide, will be listed in an implementing act based on Art. 14 OD Directive. At the time of creation of this report, the implementing act is not known yet. However, its significance for presented analysis is undisputable, because as can be seen from the Annex I of the directive, the list of general categories includes "*Companies and company ownership*". Any obligation to provide specific data from this area will be crucial especially in the context of personal data protection rules, as will be discussed further.

Apart from the general legal framework of PSI re-use, there are area specific legal instruments, with priority application, due to the general legal doctrine of *lex specialis*.[37] Examples of such cases

[31] Recital 36 OD Directive.
[32] Art. 1 para. 1 letter b) OD Directive.
[33] Art. 10 OD Directive
[34] Art. 5 para. 5 and 6 OD Directive.
[35] Art. 1 para. 6 OD Directive. More about this topic in chapter 3.3 of this report.
[36] Recital 68 of the OD Directive states: "*An Union-wide list of datasets with a particular potential to generate socioeconomic benefits together with harmonised re-use conditions constitutes an important enabler of cross-border data applications and services. …*"
[37] The principle states that if there are more laws that govern the same factual situation, the one which governs a more specific subject matter will be applied.

are directive INSPIRE[38] in the case of spatial information, or directive No. 2010/40/EU[39] and its implementing acts,[40] which regulate transport and traffic data. However, as these areas lay beyond the scope of this report, they are not discussed in any further detail.

2.3 Future and anticipated legislative actions

Currently, we find ourselves in the midst of ongoing European reform of legal regulation of data. We can include into this movement several already existing legal documents, like regulation no. 2016/679, General Data Protection Regulation,[41] or already mentioned OD Directive. However, as can be seen from publicly available documents, we can expect a lot more in this area. In February 2020, the Commission published A European strategy for data, a policy document which foreshadows future legislative attempts in the area of legal regulation of data.[42] The aim of the strategy is to create a single digital space that enables the efficient sharing and use of large amounts of data from both public and private domains. Infrastructures for the data economy should emerge - large repositories that enable efficient big data analytics and machine learning. In return, organisations providing data would gain access to the data of others. At the same time, conflicting interests (privacy, trade secrets, etc.) need to be protected. The Commission identified several issues that hinder the potential of highly efficient data handling like low availability of data, imbalances in market power, low data interoperability and quality or low skills and data literacy on the side of data re-users and general public.

The first proposal following on the European strategy for data was proposal for a regulation on European data governance (Data Governance Act, "DGA") presented by the Commission in November 2020. The final act was enacted in May 2022 as Regulation 2022/868 on European data

---

[38] 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).

[39] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance.

[40] Commission Delegated Regulation (EU) 2015/962, of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services, Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services, Commission Delegated Regulation (EU) No 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 and Commission Delegated Regulation (EU) No 885/2013 of 15 May 2013 supplementing ITS Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of information services for safe and secure parking places for trucks and commercial vehicles.

[41] And related legislature like directive No. 2016/670, regulation No. 2018/1725 and proposal for ePriacy regulation.

[42] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data. Brussels, 19. 2. 2020, COM(2020) 66 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

governance and amending Regulation (EU) 2018/1724 (Data Governance Act).[43] It consists of 9 chapters comprising 38 articles. The regulation aims to facilitate data sharing (personal and non-personal data) in the EU by making public administration data more accessible and by strengthening trust in data sharing intermediaries whose services are expected to be used in different data spaces. These include situations where public sector data needs to be made available for reuse where the data is subject to the rights of others, business-to-business data sharing for a fee in any form, the possibility to use personal data with the help of a 'data intermediation services' to assist individuals in exercising their rights under the General Data Protection Regulation and, last but not least, the possibility to provide data for altruistic reasons. The regulation does not create any new duties to provide specific data, or to process them in a specific way. It could be argued that the regulation is a meta-regulation which aims to create a trusted and secure space for sharing and managing different data. The regulation is focussed on three main regulatory areas: i) re-use of PSI which lies outside of the scope of OD Directive, ii) securing rules for creation of a safe and trustworthy data intermediation services, iii) creating safe environment for data altruism. In the context of this report the most important of them is the first mentioned, which is present in the Chapter II of the regulation.

Chapter II focuses on public sector data which do not fall within the scope of the OD Directive, because they are subject to the rights of others, such as trade secrets, statistical confidentiality, third party intellectual property rights, or their publication would constitute an infringement of data protection law. If approved, DGA will contribute to the creation of an internal market for data by facilitating the emergence of new services through a set of harmonised provisions which the Commission believes will make it easier for them to operate across borders. At the same time, like the OD Directive, it does not impose a direct obligation to provide specific data. It is left to Member States to decide what data will be made available this way. DGA, built on the FAIR data principles,[44] only sets a minimum standard of quality and principles for access to the data so identified.

Chapter II of DGA is built on the same principles as OD Directive and together they will create a complex codified environment setting the EU-wide minimal common denominator for legal regulation of PSI access and re-use. Art. 4 of the regulation prohibits exclusive arrangements between data provider and data re-user, with a possibility of exception in the cases of necessity for the provision of a service or the supply of a product in the general interest that would otherwise not be possible. Art. 5 sets basic rules of how the information should be provided. Art. 6 deals with the question of fees, and from what can be seen from the regulation, the regulation is

[43] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)
[44] For more info see e.g. https://www.go-fair.org/fair-principles/.

much more liberal than in the case of OD Directive. Art. 7 and 8 then introduce a envisaged system of competent bodies and creation of a national single information point which will help with accessing the information.[45]

DGA is a general regulation, which presents a set of rules identical to any data regardless of a specific areas or data spaces. We can expect more proposals governing area specific data in future months.

2.4 Chapter outcomes

This report focuses on international and European level of legal instruments, because they can show basic outlines and context of relevant legal regulation, which is shared among EU member states. Based on this presumption it is possible to conclude this chapter with stating that on the international law level there is no effective single shared legal framework covering access to PSI. Right to access to PSI is part of freedom of speech, but the specifics of this legal concept are different in every country, with a very limited consolidation due to the case law of European Court of Human Rights. Council of Europe Convention on Access to Official Documents (CETS No. 205) might help in this regard in the future, but as of this moment, its relevance is very limited due to the small number of contracting parties. Furthermore, on the level of national law, there may be *lex specialis* legal instruments covering specific information areas. Therefore, the question of whether the specific information can be provided must be resolved on case-by-case basis in accordance with national law.

In the second relevant area, the re-use of PSI (including open data), the situation is much better on the European law level. PSI Directive set a sound standard of legal requirements for a quality of information and data publication. OD Directive has made this standard even higher. Thanks to that it is possible to expect the same minimal requirements for the data quality in all countries of the EU and EEA. It is too soon to evaluate a quality of implementation,[46] especially in the situation when some countries have not implemented the directive yet.[47] Furthermore, it can be expected that there will be some differences in the way, how the implementation is done. OD Directive sets a minimal standard, and the member states can choose to implement a higher, more open, one. Another issue, which has still to be resolved, is how precisely will the implementing act look like, and what specific high value datasets it will present. We can expect that this question should be

[45] More detailed analysis of DGA will be present in the final version of this report, as it will be more clear how the regulation will look like.
[46] Art. 18 OD Directive expects that the Commission will carry evaluation of the directive no sooner than July 2025.
[47] E.g. the Czech Republic.

resolved at the end of 2022 and it will be present in an updated version of this report in summer 2023.

3. Protection of data & Intellectual property rights

Intellectual property rights may constitute one of several obstacles, which are needed to be dealt with during publication and re-use of PSI. If there is provided a content that is protected with any kind of intellectual property rights, the provider must license it properly (if able) to ensure effective reusability of the content. On the other hand, as will be discussed further, in a lot of situations the provided content will be not protected by any intellectual property rights at all. In such cases the data provider does not need to license the content in the strict meaning of the word "license" as a conclusion of a contract that allows a third party to use content protected by intellectual property right. Furthermore, the provider cannot license the content (in the strict meaning of the word) because there is no protected content to be licenced. However, the data provider must still proclaim and set the terms of use.[48]

Relevant international normative documents consisting of multilateral treaties regarding copyright protection are:

- Berne Convention for the Protection of Literary and Artistic Works
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (WTO)
- WIPO Copyright Treaty

Relevant European Union normative documents regarding copyright and database protection are:

- Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society
- Directive 2006/116/EC on the term of protection of copyright and certain related rights (codified version)
- Directive 96/9/EC on the legal protection of databases
- Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

All European Union member states are parties to international treaties mentioned above and are bound by the European Union directives. This creates a harmonised legal framework for the whole European Union and European Economic Area of the pertinent aspects of copyright. The following analysis builds on this harmonised framework. However, it has to be noted that there are possible differences between specific legal regulation of member states.

[48] In detail see chapter 5.

3.1 Protection of plain data

Before addressing the issues of IP rights protection and their interaction with PSI and open data, it is necessary to first address the issue of the legal regime of so-called plain data.[49] Plain data are such data that are not protected by any other regimes regulating information and its use, such as intellectual property law, trade secret protection, personal data protection, handling of classified information, etc. A particularly pressing and interesting question is whether there is such a thing as "ownership of plain data", i.e. whether plain data is capable of being the subject of property rights.

There is currently no regulation at international or European level to address this issue. In legal doctrine, however, the debate about data ownership is quite lively.[50] The possibility of creating a specific "Data Producer's Right", which would at least partially resolve the issue of an absolute right to plain data, has been raised by the European Commission in its communication on Building a European Data Economy.[51] The idea behind this proposal was to increase legal certainty and encourage re-use of data and give the market motivation to create new data. However, this proposal was met with several critical voices. As Montagnani claims,[52] firstly data is very unstable object of protection due to the speed of its creation a consumption. Secondly, the proposal did not sufficiently define the "rightful producer" of data. Finally, there was a great risk in overlap between the new right and the already existing protection frameworks as copyright and *sui generis* database rights. Nevertheless, the European legislator's efforts to address these problems can be seen in the draft European Data Strategy[53] and, in particular, the forthcoming Data Act.[54]

---

[49] There is a theoretical question concerning different possibilities of data and information legal regulation. Even though the concepts of "data" and "information" are hold different meaning, the legislator quite often interchange them. Furthermore, the regulation of information (e.g. what a person can or cannot do with specific information) often primarily affects data that are in such context, that it constitutes such information. Even though this issue is important it lays beyond the scope of this research report. For this reason, at this point we are only referring to selected relevant sources that deal with the topic. On the theoretical concept of information see Pieter Adriaans, 'Information' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Metaphysics Research Lab, Stanford University 2013); Luciano Floridi, *Information: A Very Short Introduction* (Oxford University Press 2010); Michael Keeble Buckland, 'Information as a Thing' (1991) 42 Journal of the American Society for Information Science and Technology 351.

[50] See e.g. Lee A Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35 Oxford Journal of Legal Studies 91; Martin Fadler and Christine Legner, 'Who Owns Data in the Enterprise? Rethinking Data Ownership in Times of Big Data and Analytics' [2020] Proceedings of the European Conference on Information Systems (ECIS) 1; Maria Lillà Montagnani and Antonia von Appen, 'IP and Data (Ownership) in the New European Strategy on Data' (2021) 43 European Intellectual Property Review 156.

[51] European Commission, Communication on Building a European Data Economy SWD(2017) p. 13.

[52] Lillà Montagnani and von Appen (n 49) 161.

[53] Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

[54] Online: https://digital-strategy.ec.europa.eu/en/policies/data-act.

In the context of EU law, the most that can be mentioned is the Regulation on a framework for the free flow of non-personal data in the European Union.[55] While this Regulation governs certain obligations that Member States have with respect to plain data, it does not address the issue of data ownership at all. Of course, this is because the definition of ownership and the objects that are eligible for ownership is a matter of private law, which is mainly regulated at the level of national states. To the best of our knowledge, and within the limits of this report, we are not aware of a case of a jurisdiction granting the status of a thing protected by property law to plain data.[56] We cannot, of course, rule out the possibility that such an arrangement exists somewhere.[57] For this reason, it is essential to check the situation in a particular country before starting the process of providing open data. However, we consider that the presence of such an arrangement is highly unlikely.

3.2 Copyright protection

3.2.1 Legislative overview

In the context of the legal regulation of public sector information and open data, we may encounter cases where the provided content or parts thereof enjoy copyright protection. Copyright is an absolute right that protects the results of the author's creative activity (works of authorship) in such a way that it excludes anyone else[58] from any dealing with and influence on the copyright work. A work of authorship is then understood as a personal expression of a natural person, which corresponds to the dual concept of protection consisting in a combination of moral[59] and economic rights. It is worth mentioning that moral rights are not harmonized at all by the European Union directives and thus, the scope of their protection depends on legal order of each Member State.

Art. 2 section 1 of Berne Convention, a ground stone of international copyright protection, defines protected copyrighted work (or "authorial work") as follows: "*The expression "literary and artistic works" shall include every production in the literary, scientific and artistic domain, whatever may be*

[55] 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.
[56] A good overview offers Boerding in Andreas Boerding and others, 'Data Ownership - A Property Rights Approach from a European Perspective' (2018) 11 Journal of Civil Law Studies 323, 334–345.
[5757] Boerding claims that generally legal orders in European countries may support the concept of data ownership. ibid 369.
[58] It should be noted that there are exceptions and limitations to copyright. The reason for their existence is that copyright is not intended to act as a tool for the monopolization of ideas. The exceptions and limitations are then intended to ensure the further dissemination of ideas and the growth of creativity. See e.g. Christophe Geiger, 'Promoting Creativity through Copyright Limitations: Reflections on the Concept of Exclusivity in Copyright Law' (2009) 12 Vanderbilt Journal of Entertainment and Technology Law 515.
[59] Art. 6 of Berne Convention.

the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramatico-musical works; choreographic works and entertainments in dumb show; musical compositions with or without words; cinematographic works to which are assimilated works expressed by a process analogous to cinematography; works of drawing, painting, architecture, sculpture, engraving and lithography; photographic works to which are assimilated works expressed by a process analogous to photography; works of applied art; illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science." In the context of access to PSI and open data, especially literary works expressed in speech or writing, photographic works, visual works, architectural works, urban works and cartographic works are relevant.

The EU copyright law does not provide for a clear-cut general definition of the copyrighted work.[60] However, the CJEU laid down basic preconditions that an intangible creation must fulfil to be qualified as a copyrighted work.[61] The basic standard is that the work must be original, i.e., ''the author's own intellectual creation''.[62] Consequently, a work must not be copied and must be a result of intellectual creative activity of the human author.[63] The work must thus reflect personal choices of its creator. These are not present[64] when the expression is dictated by rules,[65] technical function[66] and technical considerations[67] or the information content itself[68], which disallow the creator to express her "creative abilities in the production of the work by making free and creative choices" [69] – i.e., leave no room for creative freedom. In the context of PSI it is noteworthy, that the mere fact that "mere intellectual effort and skill" were required for the creation of the intangible result are not relevant for its copyrightability.[70] Artistic merit or aesthetic quality are also not

[60] P Bernt Hugenholtz and João Pedro Quintais, 'Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?' (2021) 52 International Review of Intellectual Property and Competition Law 1190, 1193.
[61] For an extensive debate what is protected as „work" in the EU see Caterina Sganga, 'The Notion of "Work" in EU Copyright Law after Levola Hengelo: One Answer Given, Three Question Marks Ahead' (2019) 41 European Intellectual Property Review 415.
[62] As ruled in the CJEU decision of 16. 7. 2009, No. C-05/08 (Infopaq International). This requirement was adopted as the basic standard in the subsequent topical cases Levola Hengelo (CJEU decision of 13. 11. 2018, No. C-310/17), Funke Medien (CJEU decision of 19. 7. 2019, No. C-469/17), Cofemel (CJEU decision of 12. 9. 2019, No. C-683/17) and Brompton Bicycle (CJEU decision of 11. 6. 2020, No. C-833/18).
[63] Hugenholtz and Quintais (n 57) 1196.
[64] These constraints on creativity were identified by ibid 1198.
[65] E.g., a football match where the game rules are applicable (joined Cases C-403/08 and C-429/08 Premier League, para. 98).
[66] E.g., the functionality of a graphical user interface as was presented by CJEU decision of 22. 12. 2010, No. C-393/09 (Bezpečnostní softwarová asociace), para. 49-50.
[67] CJEU decision of of 11. 6. 2020, No. C-833/18 (SI and Brompton Bicycle Ltd), para. 26.
[68] CJEU decision of of 29. 7. 2019, No. C-469/17 (Funke Medien), para. 24.
[69] As required in the CJEU decisions of 19. 7. 2019, No. C-469/17 (Funke Medien), para. 19 and of 7. 3. 2013, No. C-145/10 (Painer), paras 87–88.
[70] CJEU decision of 19. 7. 2019, No. C-469/17 (Funke Medien), para. 23.

required.[71] The protection by copyright law is neither justifiable by the economic investment as such.[72] Finally, as noted by Hugenholtz and Quintais, the work must be expressed "in a manner which makes it identifiable with sufficient precision and objectivity"[73] – ideas that have not been materialized in a form or a shape are not "works".[74]

In the context of access to the information frequent relevant examples of works, such as various analyses and expert opinions, but may also include other copyrighted works, as in the case of works held by libraries and museums.[75] In the context of open data, copyrighted works may appear either as part of a provided dataset or the dataset itself may be a work. An example of the former is a database of entries to a literary competition organised by a local authority, or a database of expert opinions commissioned by a public authority on various issues.[76] As another practical example can be mentioned database of tourist destination run by a public sector entity "Czech Tourism"[77] that includes photos and descriptions of interesting places and destinations. An example of the second variant could be a map documentation, which is a cartographic work.

In addition to the above examples, a database itself may be protected as a copyrightable work. This follows from Article 3 of Directive 96/9/EC which states: "*In accordance with this Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection.*" Database is 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*".[78] It is important to note that copyright protects the structure of the database, i.e. the selection and arrangement of the content. The content itself is not protected in this way.[79]

The author of the database is the person who organised the content. The conditions for granting copyright protection to a database are therefore that: a) it is the author's own intellectual creation; b) the selection of the elements and their arrangement must be the result of creative activity. As

[71] Hugenholtz and Quintais (n 57) 1197.
[72] Ibid.
[73] CJEU decision of 13. 11. 2018, No. C-310/17 (Levola Hengelo), para. 40.
[74] Hugenholtz and Quintais (n 57) 1199.
[75] The goal of ensuring reusability of content held by, e.g., public libraries was one of the main legislative aims of 2013 PSI directive amendment.
[76] In this variant, the difference between the work itself and the metadata that describes it must be taken into account. Only the work itself would be copyrighted, but the dataset would certainly include metadata such as the identity of the author, date of publication, etc., which are not protected.
[77] In Czech online: https://www.kudyznudy.cz/.
[78] See Art. 1 (2) Directive 96/9/EC.
[79] See Art. 3 (2) Directive 96/9/EC.

Hugenholtz points out,[80] the first condition was clearly addressed by the Court of Justice of the European Union in Case C-604/10 (Football Dataco), in which it held that "*criterion of originality is satisfied when, through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices … and thus stamps his 'personal touch'.*"[81] This criterion is not met "*when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom*".[82] The second condition (the selection of elements is a creative activity) is very well demonstrated by Hugenholtz's example, according to which a list of the author's favourite restaurants in Amsterdam could enjoy protection, while a list of the most expensive restaurants probably would not.[83] A database that meets the above conditions for granting copyright protection is referred to as an "original database".

Some jurisdictions may cover an exception of official work. Generally, this exception ensures that certain content, that would otherwise fulfil the criteria of copyrighted work, is not protected by copyright, because of its importance for public interests. For example the Czech copyright act covers such exception as follows: "*Protection under copyright law does not apply to an official work, which is a legal regulation, a decision, a measure of a general nature, a public document, a publicly accessible register and a collection of its documents, as well as an official draft of an official work and other preparatory official documentation, including an official translation of such a work, parliamentary and senate publications, commemorative books of a municipality (municipal chronicles), a state symbol and a symbol of a unit of local self-government, and other such works for which there is a public interest in exclusion from protection.*"[84] The possible existence of such exception is quite important, because if the provided content (which would otherwise fulfil the criteria of copyrighted work) falls within its scope, it can be provided and further reused without any obstacles and without a need for any licences.

3.2.2 Copyright and open data

When it comes to the context of the publication and re-use of PSI that is in some way encumbered by third-party copyright, even though these situations will not in fact be very common, there are two areas which must be taken into account. Firstly, the distinction between access and re-use is absolutely crucial. In the event of a conflict with copyright, there may be a situation where, based on certain copyright limitations or exceptions, information can be disclosed even though it is

[80] P Bernt Hugenholtz, 'Directive 96/9/EC' in Thomas Dreier and P Bernt Hugenholtz (eds), *Concise European copyright law* (Second edition, Kluwer Law International 2016) 392 <https://media.wolterskluwer.com/pdfs/SampleChaptersPDF/6651.pdf>.
[81] Para. 38 of CJEU case No. C-604/10 (Football Dataco and Others).
[82] Ibidem, para. 39.
[83] Hugenholtz (n 77) 393.
[84] Sec. 3 letter a) Act. No. 121/2000 Sb., copyright act. Translation by the authors.

copyrighted. For example, some states have enacted an exception for the use of a work for an official purpose. The disclosure of information is undoubtedly a fulfillment of the official purpose, as it is a decision about the right to information (and thus, by implication, the right to freedom of expression). If the disclosure of a copyrighted work is proportionate and passes the three-step test as defined, for example, by the Berne Convention, the obliged entity may disclose the work to the applicant upon request. However, this does not mean that the applicant can freely continue to use it without further permission, as the statutory licence no longer entitles him to do so. Thus, the applicant may, at most, make use of other legal grounds (statutory licences and copyright limitations), but may not redistribute or exploit the work in any other way without further permission. For this reason, relying solely on exceptions for further use of PSI is inappropriate, and if any of the content provided is copyrighted it is necessary to license it (see more later in Chapter 5 of this research report).

The second area is connected to the copyrighted databases. When providing open data, it is possible to encounter copyrighted original databases. We think that this is more likely to be the case when the obliged entity creates the database and provides data on a discretionary basis, because in the case of mandatory provision, the selection of elements in the database is determined by law and therefore lacks room for creative freedom. However, even for these databases, protection can be achieved due to the possibility of original arrangement of the elements prescribed by law. This is even more true, when there are present more complex database structures, which interconnect multiple information resources. With regard to the scope of STIRData project, we can assume that a majority of concerned databases will be protected by a copyright, more specifically their structure will be protected. However, that does not necessarily mean that the protection will apply also on the open data export of the content of such databases. The export can be in a different structure than in the source database, and in such case the copyright protection of the source database would not be infringed. The same goes for the situations, when the data re-user accesses the source database via an API. Again, it the data are later stored in a different structure than was the original, its copyright protection would not be infringed. However, a different outcome might be in a situation where the copyright protection is constructed thanks to the way of selection of the contents of the source database. In every case, should there be a copyrighted content, the open data provider should publish it only under a proper open licence.[85]

[85] More on this topic see chapter 5 of this report.

3.3 Sui generis database rights

The sui generis database right, or the right of the maker of the database, has its roots in the European Directive 1996/9/EC. As can be seen from its recitals 10 to 12, the main purpose of the sui generis database right is to protect the investment made in its creation.[86] The above-mentioned definition of a database[87] applies not only to the case of an original copyrighted database, but also to databases protected by *sui generis* right. This also means, that the same database can be protected by both means, either of them, or none of them.[88] In other words, copyright protection of a database is entirely independent on the protection by *sui generis* rights.

The maker of the database is defined as a person who takes the initiative and the risk of investing.[89] This is the first fundamental difference from copyright, because if a database provided by a third party achieves the conditions for the creation of a *sui generis* right, this right is created directly for the customer and not for the external provider (e.g. IT company which provides database solutions for the public sector body). As Hugenholtz points out, in order to be granted the status of a maker of the database, it is essential that the entity in question both invested in the creation of the database and instigated its creation.[90]

The right itself is defined in Art. 7 of Directive No. 96/9/EC as right to "*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*". Even though the main purpose of sui generis right is to protect the investment in the database,[91] it is clear that through this right is affected the content of the database, regardless of whether the content itself is protected in any other way. This is an absolute right, so no one can without a permission interfere with it by extracting or re-utilizing a substantial part of the database. Furthermore, the protection applies not only on the primary database, but also on the copies and exports of the database.[92] However, the maker may grant another person the right to exercise this right with a license.

The term extraction is practically identical with the concept of copying of the database content. A broad interpretation also leads to the conclusion that the application of the concept will also include, for example, the creation of temporary copies for the purpose of displaying the database

---

[86] See also Hugenholtz (n 77) 402.
[87] Art. 1 (2) directive 96/9/EC reads as follows: "*database shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means*".
[88] See CJEU decision of 15. 1. 2015, No. C-30/14 (Ryanair Ltd v PR Aviation BV).
[89] Rec. 41 directive 96/9/EC.
[90] Hugenholtz (n 77) 403.
[91] See CJEU decision of 3. 6. 2021, No. C-762/19 ('CV-Online Latvia' SIA), in which the court stated that extraction and re-utilization of the content within the meaning of the provision of Art. 7 is when there is a "*risk to the possibility of redeeming … investment through the normal operation of the database in question*".
[92] See para. 52 of CJEU decision of 9. 11. 2004 No. C-203/02 (The British Horseracing Board).

on a computer screen, whereby this activity is not covered (unlike copyright) by any of the exceptions to the sui generis database right of, with the result that such activity should be subject to the consent of the maker of the database.[93]

The term re-utilizing means any activity that makes the contents of the database available to the public. In the Innoweb decision, the Court of Justice of European Union (further CJEU) held that the operator of a "metasearch engine", a service that redirects users' queries to other search engines and offers the user results from specialised databases through this process, re-utilizes the content of those databases and their substantial parts.[94]

For example, in the context of open data, database extraction is the downloading of a copy of a database file to the data storage of the data re-user. Database re-utilisation is then the creation of an application that interacts with the database and allows third parties to access its contents, e.g. via API.

It follows from the above that the *sui generis* database right of the database maker indirectly protects the content of the database. However, it does not protect individual data, but only becomes applicable when a substantial part of the database is affected. Unlike copyright, the *sui generis* right does not have a personality component, can be waived and is transferable.[95]

Directive 96/9/EC states in Art. 7 (1) that *sui generis* database right protects a database "*which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents*". A quantitative investment is one that consists of quantifiable resources, such as time and money.[96] On the other hand, a qualitative investment consists of non-quantifiable effort, such as mental effort or energy expended. Hugenholtz gives an example of the use of a web designer's skills in creating an online database or a lexicographer's knowledge in creating keywords as examples of qualitative input.[97] The assessment of when a investment is "substantial" must be made on a case-by-case basis. However, it is not entirely clear when the investment is sufficiently substantial, i.e. what the threshold for a substantial investment is.[98] Slightly helps the wording of recital 19 of the directive which reads that "*… as a rule, the compilation of several recordings of musical performances on a CD does not come within the scope of this Directive, both because, as a compilation, it does not meet the conditions for copyright protection and because it does not represent a substantial enough investment to be*

[93] See Hugenholtz (n 77) 406.
[94] CJEU decision of 19. 12. 2013 No. C-202/12 (Innoweb).
[95] See Art. 7 para. 3 Directive No. 96/9/EC.
[96] See recitals 7, 39 and 40 of the Directive 96/9/EC and para. 44 and 46 CJEU decision of 9. 11. 2004, No. C-338/02 (Fixtures Marketing Ltd v Svenska Spel AB).
[97] Hugenholtz (n 77) 404.
[98] Ibidem.

eligible under the sui generis right" and recital 7 which reads that "*... the making of databases requires the investment of considerable human, technical and financial resources*". The case law of the CJEU did not help in this matter either.

Substantial investment must be made in the obtaining, verification or presentation of the contents of the database, taking into account the total input to these three components. Obtaining consists of locating existing independent elements and placing them in the emerging database. However, the Obtaining costs do not include the costs necessary to create the elements.[99] The content verification criterion consists of the resources expended by the database builder to verify the veracity and accuracy of the data already present in the database. The investment in the presentation of the database content consists of an investment in resources in "*the resources used for the purpose of giving the database its function of processing information, that is to say those used for the systematic or methodical arrangement of the materials contained in that database and the organisation of their individual accessibility.*"[100] Hugenholtz mentions the digitisation of analogue files, the creation of a thesaurus or user interface design as examples of such activity.[101] In our opinion such an activity could also be the creation of an application programming interface (API) that can be used to access the contents of the database in an automated way. A practical example of a substantial investment in demonstrating content in the context of open data seems to be the cost of 2,000,000 CZK incurred by the Ministry of Finance in modifying the ARES register[102] to allow open data to be published from it.[103]

OD Directive brought a major change in the context of *sui generis* database right and its application during PSI and open data publication and its reuse. As mentioned earlier, Art. 1 (6) OD Directive states: "*The right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC 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 this Directive.*" For a time, it was even disputed, whether public sector bodies can acquire *sui generis* database right. Its purpose is to protect the investment in the database and public sector body generally does not need that, as it manages only public money, it creates databases only to fulfil legal duties and thus there is not a risk in the investment.[104] The

[99] See Hugenholtz (n 77) 405. In the same manner see para. 42 of CJEU decision of 9. 11. 2004 No. C-203/02 (The British Horseracing Board) and para. 53 CJEU decision of 9. 11. 2004, No. C-338/02 (Fixtures Marketing Ltd v Svenska Spel AB).
[100] Para. 43 CJEU decision of 9. 11. 2004, No. C-338/02 (Fixtures Marketing Ltd v Svenska Spel AB).
[101] Hugenholtz (n 77) 405.
[102] Register of Economic Subjects which, which contains data from registers of persons, company ownership and more.
[103] Slížek D. Dodám vám systém na otevření dat ARES za 1 Kč, nabízí ministerstvu Michal Bláha. Lupa.cz [online], 2017 [seen 31. 10. 2022]. Online: https://www.lupa.cz/aktuality/dodam-vam-system-na-otevreni-dat-ares-za-1-kc-nabizi-ministerstvu-michal-blaha/.
[104] Hugenholtz states that on the basis of this argument the Dutch Raad van State refused to recognise a sui generis database right of the City of Hamburg. See Hugenholtz (n 77) 405.

provision of Art. 1 (6) pragmatically reflects practice in the member states, which allow for such protection to exist. However, at the same time it effectively cancels any possibility to enforce *sui generis* database rights in a way that would prevent any kind of future re-use of the data. Therefore, the data providers must licence or waive[105] the *sui generis* right when they publish the protected database.

At first sight, it may seem that this entire chapter, which has dealt in detail with the *sui generis* database right, is superfluous because of the impossibility of enforcing this right. And that it would suffice to simply state that EU law shows that this right cannot constitute an obstacle to further use of PSI. However, the provision of Art. 1 (6) OD Directive does not preclude existence of such right. Therefore, if the database of public sector body (or another data provider falling within the scope of OD Directive) fulfils the requirements of substantial investment in the obtaining, verification or presentation of its contents, the *sui generis* database right will objectively exist, and it will protect such database. It is necessary to properly licence such databases for the sake of legal certainty of re-users. Without a correct license, re-use of the protected database in the context of open data applications and further activities would be illegal, regardless of the provision of Art. 1 (6) OD Directive.

3.4 Chapter outcomes

When providing open data, it is possible to encounter several legal obstacles related to the content provided, created by intellectual property rights. These obstacles need to be overcome by proper licensing, as without it, unlimited re-use of the provided data is not possible. First of all, it should be noted that most of the content provided as part of open data from public registers will be in the form of 'plain data'. Plain data is when it is of such a nature that it is not subject to any specific form of legal protection, such as intellectual property rights, trade secrets, personal data, etc. The legal assessment of plain data may vary from jurisdiction to jurisdiction as there is no European or international harmonisation of plain data. Within the scope of the limitations of this research report, it can be concluded that plain data is not protected by property law and therefore not subject to absolute rights of ownership. In view of this, there is no legal barrier present that would per se limit their provision and re-use.

In the area of intellectual property rights, the chapter identified three rights that may be relevant in the provision and re-use of PSI and open data. The first is copyright protection of the content of the database provided. This will be a relatively atypical and minority case because it requires that

[105] A waiver of the *sui generis* database right should be applicable in the most jurisdiction of EU and EEA member states. It is not excluded in the directive 96/9/EC and since the database right stems directly from this directive, it is safe to assume that national legislators did not include this kind of exclusion.

the content provided meets the standard for a copyrighted work. However, if such a situation does happen to arise, it is essential to license the content properly.

The second is the copyright protection of the database itself. In this case, it is protected in particular its structure and the way its content is selected. In the case of public databases, protection will be based on the structure of the database, where the intellectual work of its creators is protected, rather than on the selection of its content. This is because the content will often be based directly on the requirements of the legislation and the choice of content will therefore not offer scope for the intellectual activity itself. Copyright protection of a database does not protect the content as such. It is therefore theoretically possible to allow the sharing and re-use of content without the need for licensing, as long as this does not also copy the structure of the source database. Nevertheless, in order to ensure legal certainty, we recommend that the database be properly licensed if this right exists.

The third is the sui generis rights of the database maker. Although this protection is mainly concerned with the investment made in the source database, it also indirectly affects the content of the database. Where content is provided from a database protected by sui generis database rights, it must be licensed, otherwise the recipient will be restricted in its further use of the data provided. This requirement then also follows directly from Art. 1(6) of the OD Directive, which states that sui generis database rights must not constitute an obstacle to the further use of the data provided.

All three types of protection can be combined. At the same time, it is quite common that the dataset provided is not protected by any of these rights. The assessment of the presence of protection should be made on an ad hoc basis directly by the open data provider before the provision of open data. The details of how to license the content are discussed in Chapter 5 of this research report.

4. Personal data protection

4.1 Privacy a personal data protection: Overview of the regulation

4.1.1 Introduction to the topic and overview of relevant legal instruments

The right to privacy and personal data protection has traditionally been in conflict with the right of free access to information and its re-use. This situation stems from the very basic principles underlying the rights in question. While the right of access to information respects the essential character of information and presupposes its dissemination in accordance with the principle of publicity, the protection of privacy and, in particular, the protection of personal data requires the opposite. This is particularly true for personal data protection, whose system is based on the prevention of damage, the control of data and ensuring that they are not used in violation of the rights of data subjects.[106] Both PSI and Open Data Directives are aware of this collision and therefore they include provision stating, that the directive is without prejudice to Union and national law on the protection of personal data.[107] This does not mean, that personal data cannot be provided in open data quality. However, when dealing with publication and re-use of PSI, it is still necessary to take into account the whole personal data protection legal framework.[108]

One of the basis for the right to data protection is the right to informational self-determination.[109] This guarantees every person the possibility to determine how information about their person will be treated.[110] This is not an absolute right and there are exceptions to it, for example in the form of the processing of information by state authorities. In general, however, the right to informational self-determination gives each person the possibility to determine how he or she will present him or herself in public, what information he or she wants to be known about him or her and, ultimately, what information he or she wants to receive.

Data protection legislation pursues two objectives. The first is to ensure that the right to protection of personal data of natural persons (data subjects) is not infringed. Data protection

---

[106] See e.g. Raphaël Gellert, 'Understanding Data Protection as Risk Regulation' (2015) 18 Journal of Internet Law 3.

[107] See Art. 1 section 4 Open Data Directive.

[108] For a general overview see e.g. Cristina Dos Santos, 'On Privacy and Personal Data Protection as Regards Re-Use of Public Sector Information (PSI)' (2013) 6 Masaryk University Journal of Law and Technology 337; Frederik Zuiderveen Borgesius, Jonathan Gray and Mireille van Eechoud, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework' (2015) 30 Berkeley Technology Law Journal 2073.

[109] See e.g. Theo Hooghiemstra, 'Informational Self-Determination, Digital Health and New Features of Data Protection' (2019) 5 European Data Protection Law Review 160; Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the Eu Legal Order' (2014) 63 International & Comparative Law Quarterly 569.

[110] The right was i.a. grounded by the decision of German Federal Constitutional Court from 15. December 1983 No. BvR 209/83, BVerfGE65, which concerned a case of publication of unsatisfactorily anonymised dataset of public census.

legislation regulates the behaviour of obliged entities in relation to the personal data they process. If someone decides to handle personal data, in the vast majority of cases, processing will take place. As a consequence, the data controller must comply with the obligations arising from the legislation. From the point of view of data protection law, it does not fundamentally matter too much who the personal data belongs to.

Data protection law regulates how personal data is treated. It is a preventive instrument, based on the premise that if the data controller complies with the obligations imposed on him, the risk of damage, harm or misuse of personal data caused by the processing is reduced. As a result, other fundamental rights that could be affected by the mishandling of personal data are indirectly protected. First of all, the right to privacy, as the risk of disclosure of sensitive information about a person is limited when personal data is handled properly. However, further examples of rights indirectly protected in this way include the right to property (the mishandling of personal data can lead, for example, to identity theft and misuse of payment cards) or the prohibition of discrimination (discriminatory practices can occur on the basis of the mishandling of personal data). Data protection law is essentially like an umbrella protecting other rights that could be violated by the processing of personal data.

The second objective of the legislation is generally to enable processing of personal data that is lawful and that respects the protection of the rights of data subjects.[111] Data protection legislation is pragmatic because it is based on the assumption that the processing of personal data happens and is generally appropriate for society to do. A popular saying claims that personal data is the new oil because it enables economic exploitation and progress. Data protection legislation is therefore not intended to prohibit the processing of personal data altogether. Processing is generally possible as long as the data controller approaches it responsibly so as to minimise the risks that the processing may pose to the data subject. The two objectives mentioned above are dynamically complementary. The object of any processing of personal data is to strike a balance between them.

Legal instruments regarding personal data protection on international level relevant for this analysis are:

- European Convention for the Protection of Human Rights and Fundamental Freedoms
    - Art. 8 protects right to a private and family life

[111] See e.g. Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001); Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 3.

- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

Legal instruments regarding personal data protection on European Union level relevant for this analysis are:

- Charter of Fundamental Rights of the European Union (Document No 2010/C 83/02)
    - Art. 8 reads as follows:
      "*Protection of personal data*
      1. Everyone has the right to the protection of personal data concerning him or her.
      2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
      3. Compliance with these rules shall be subject to control by an independent authority."
- 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 (General Data Protection Regulation, further "GDPR")
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

4.1.2 Overview of basic concepts

In this section are presented basic concepts, which are necessary for the following legal analysis.

The term "**personal data**" is defined in Art. 4 para. 1 GDPR 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*". Personal data is really any information that can directly or indirectly lead to the identification of a natural person. Personal data protection legislation does not apply to legal persons. Directly identifying personal data is information or records which, directly from their own context, are clearly capable of identifying a person. This includes, for example, a name, a permanent residence, an identity card number or a telephone number. Indirectly identifying data are, on the other hand, data that cannot lead to identification on their own, but if combined with other data in the right

context, can already be used to identify a person. The definition of personal data is extremely broad due to this definition, as it can cover a really large amount of information. This includes, for example, IP addresses that identify users' personal devices, which can be used in criminal investigations. It should be stressed that indirectly identifying personal data is indeed personal data even if a specific data controller cannot use it to identify a specific person at the time. CJEU set in the Breyer decision (C-582/14) the limits of scope of what is personal data that it is no longer personal data if "*the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant*".[112] This is essential for the notion of anonymisation.

Anonymous data is data that has undergone a process of irreversible anonymisation and can no longer be used to identify a specific person. Therefore, they are no longer considered personal data.[113] However, it is more appropriate to think of use of anonymisation techniques as a scale between identification and absolute anonymity, because the more anonymous the data, the less informative it is, and vice versa.[114] Based on the results of Breyer case, we can consider as anonymous data that would clearly be disproportionately difficult or costly to re-identify given the state of the art. Furthermore, in the context of open data, there is always a risk of re-identification, because of the free access to the data and possibility of its re-use and connecting with other datasets. Moreover, the evolving technology may also allow re-identification of datasets in instances, where it was previously not possible.[115]

Pseudonymous data are those where direct identifiers are replaced by indirect identifiers.[116] This is for example the substitution of a number for a name and surname. However, as the above shows, it is still personal data, albeit more secure. Generally, we can say, that application of anonymisation techniques on a dataset creates pseudonymous data and once it is practically impossible to reidentify original data subjects, we can consider it anonymous data. It is useful, especially in the context of open data publication and re-use, to consider anonymity and pseudonymity as a scale, and not as a number of discrete states. The following figure shows this relationship:

---

[112] See para. 46 CJEU decision of 19. 10. 2016 No. C-582/14 (Breyer).
[113] See recital 26 GDPR.
[114] Similarly see Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.
[115] For more information on anonymisation and its legal consequences and shortcomings, see e.g. Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701.
[116] Art. 4 para. 5 GDPR.

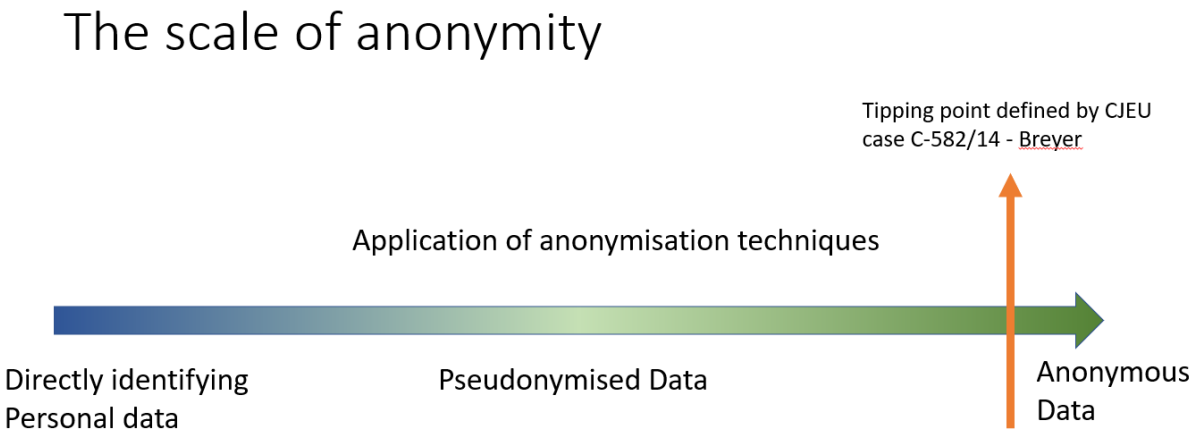

Figure 1 The scale of psudonymity and anonymity

Special categories of personal data are defined and enumerated in Art. 9 GDPR. It includes "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" and its processing is generally prohibited, unless one of specific exemptions listed in Art. 9 para. 2 applies. This is because these categories of personal data pose an increased risk for data subjects and their rights, because of their possible discriminatory nature. Generally special categories of personal data cannot be published as PSI (not to mention in open data quality) because it would constitute too great an interference with the rights of data subjects.[117]

Data controller is defined in Art. 4 para. 7 GDPR as "*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*". The purpose of the processing is an absolutely essential element in the context of the entire legal framework for the protection of personal data. The purpose that the controller has identified at the beginning of the processing is then measured against how to ensure that the processing can lawfully take place, how long the data can be kept, who can have access to it and so on.[118] The data controller often processes data for different purposes and is thus accountable for multiple processing processes.

Data processor is defined in Art. 4 para. 8 GDPR as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". The main difference between data controller and processor is that data processor does not set the purpose of processing but has to follow the purpose set by the controller.

[117] See CJEU decision of 22. 6. 2021 No. C-439/19 (Latvijas Republikas Saeima).
[118] Art. 5 para. 1 GDPR.

Personal data processing is defined in Art. 4 para. 2 GDPR as "*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*". As with personal data, the definition of processing is extremely broad. In general, it is any activity that a controller or processor carries out with personal data during its life cycle. It is useful to think of processing of personal data procedurally over time. Thus, a single processing process, which is defined by an identified purpose, may comprise several sub-activities of handling personal data.

Art. 5 GDPR enumerates **basic principles** relating to the processing of personal data, which are applicable in every instance of personal data processing. In the context of this general overview, the most important are the principle of lawfulness, fairness and transparency,[119] principle of purpose limitation,[120] principle of storage limitation,[121] and principle of accountability.[122]

An important part of principle of lawfulness is a requirement to rely on a specific **legal ground** for data processing, without which the data controller cannot even start with the processing. These legal grounds are listed in Art. 6 para. 1 GDPR. For the context of this analyses, the only legal grounds which are relevant for publication and re-use of PSI (and open data) are fulfilling a legal obligation to which the controller is subject,[123] performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,[124] and legitimate interest pursued by the controller or by a third party.[125] Other legal grounds are not applicable in the context of publication or re-use of PSI.

4.2 Open data as personal data processing

OD Directive, similarly to its predecessor, sets in its Art. 1 para. 2 letter h) that it does not apply to the "*documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data*". This provision sets a hard

[119] Art. 5 para. 1 letter a) GDPR.
[120] Art. 5 para. 1 letter b) GDPR.
[121] Art. 5 para. 1 letter e) GDPR.
[122] Art. 5 para. 2.
[123] Art. 6 para. 1 letter c) GDPR.
[124] Art. 6 para. 1 letter e) GDPR.
[125] Art. 6 para. 1 letter f) GDPR.

line of the relation between PSI (and open data) and personal data protection. The specific implementation of this legislation is then up to individual EU Member States, some of which, such as Germany or Belgium, require complete anonymisation of personal data, while others allow further use of personal data disclosed in this way on the basis of legal authorisation (for example, France, Slovenia and the Czech Republic).[126]

More of a theoretical question is whether personal data can be ever published as open data at all. This question relates to the fact that traditionally the term "open data" means data provided without any legal restrictions. At the same time, processing of personal data in the European context will always present some kind of a restriction arising from the relevant legal framework, GDPR in particular, because data subjects cannot waive their rights. Therefore, it may seem, that personal data cannot ever be published as open data (or in open data quality).

In our opinion, it is necessary to understand the concept of open data in the broader context of European law. Should the stricter interpretation (that is that "open data" must be without any restriction) be true, not even databases containing licensed copyrighted content, could be considered open data, as there will be residual duties to attribute the work, since in many jurisdictions the author cannot waive their rights. Furthermore, as can be seen from the activity of European legislator, who put data concerning business ownership into the Annex I of OD Directive, it is clear, that the legal context of the open data concept needs to be adjusted for the European reality. Therefore, the principle that open data must be provided without any legal restriction needs to be interpreted in a way, that the data provider cannot impose new legal restrictions and must do their best to minimalise restriction arising from the statutory law.

Regardless of this theoretical question, it is necessary to note, that there might be practical legal consequences in the approach of the legislator and the decision how they will publish a dataset with personal data. For example, legally describing a published dataset with a notion of open data or stating expressly that that the dataset is purposed for further reuse, will help the re-users to bear the burden of proof in regards to the legal ground of their new data processing.[127]

In the context of open data, we distinguish between two types of data controllers. The first are data providers, who usually process information containing personal data (by making it public) on the basis of a legal obligation. The purpose of such processing is therefore for the purpose of the relevant legal provision or directly to fulfil that obligation. It is also theoretically conceivable for data providers to process data for a purpose of their own choosing (for example, voluntary information to the public). However, in the case of such processing, it is quite difficult to ensure

[126] Santos (n 104) 338.
[127] This will be more discussed further in part 4.4 of this report.

its lawfulness, as will be discussed in detail later in this section. The second type of controllers are open data re-users. These are usually private entities, app developers or individuals who want to use the data to inform themselves about the issue. The purposes of processing published personal data can vary widely and it is up to these new data controllers to determine them in accordance with GDPR and to comply with all the obligations imposed on them by data protection legislation.

4.3 Open data provider as data controller

Where an open data provider, whether a public sector body or a public undertaking, provides personal data in open data format, it is clearly in the position of a data controller and therefore they have to fulfil the obligations arising from GDPR. In the following considerations, several variations of the situation have to be taken into account. Firstly, the question of whether at all and when a data provider can publish personal data must first be addressed. Only when these cases are identified can one consider whether it is possible to provide it in a more qualitative way, i.e. as open data.

The first fundamental question is whether an open data provider can decide, at its discretion, to publish personal data. This issue is directly following a question addressed in the chapter 2 of this report, whether the data provider has a legal capacity to provide the data in general. If the data provider were to provide personal data on a discretionary basis as open data, it would first have to determine the appropriate purpose of such processing of personal data and to base such processing with one of the legal grounds in accordance with Art. 6 GDPR. Determining the purpose for such processing is difficult, but not impossible. This could be, for example, to ensure law and security in the case of the publication of a list of dog owners by a municipality, or for transparency where lists would be provided with information on the recipients of benefits and aid that the municipality has decided to pay. However, for most of these examples, GDPR does not offer a legal ground for such processing of personal data. As these would be voluntary disclosures, not directly based on law, or which would have to be made in the course of the performance of public authority tasks, the legal grounds of Art. 6 para. 1 letters c) and e) cannot be applied. Nor is it possible to rely on the legitimate interest listed in Art. 6 para. 1 letter f), because this legal ground cannot be used to processing carried out by public authorities in the performance of their tasks. Theoretically the data provider could acquire consents od the data subjects and later rely on the legal ground listed in Art. 6 para. 1 letter a), but this option will be not achievable for practical and technical reasons in most of the situations. Therefore, we can conclude that it is not possible to publish personal data as open data voluntarily based on a discretion of data provider and thus this possibility stays out of the application scope of OD Directive.

One way, how to overcome this problem, is anonymisation. The data provider, most likely the public sector body which holds an interesting database, might be able[128] to conduct anonymisation of the data and publish it as statistics. Once the data are anonymous, therefore it would clearly be disproportionately difficult or costly to re-identify given the state of the art,[129] data provider can publish it online. However, the anonymisation process must be done very diligently, due to the risk of reidentification[130] and possible further high risk to rights and interests of data subjects.

The situation is different when the data provider has a legal obligation to provide personal data as PSI (or directly as open data).[131] In this situation will be OD Directive applicable. However, even in these cases, the data provider is in the position of a personal data controller. The purpose of such processing (provision of data) stems from the law under which the processing is carried out. In the case of the above example, the purpose is, for example, transparency and ensuring the possibility of contacting the persons responsible for the management of the commercial company. The legal titles for the processing of personal data in these cases will be processing resulting from a legal obligation or the performance of a task carried out in the public interest or in the exercise of official authority within the meaning of Art. 6 para. 1 letters c) and e) GDPR. A legal obligation imposed on the data provider is therefore necessary for the possibility of publishing personal data. It should be stressed that the processing in question is always strictly limited to the purpose and wording of the enabling legislation.

When the data provider publishes personal data, the technical means by which such publication is made matters enormously in terms of ensuring the protection of the rights of data subjects.[132] In terms of potential interference with the right to privacy, it makes a difference whether the information - personal data - is provided in the form of a freely downloadable complete database file (with open data being only a better version of this) or whether the individual data are only

---

[128] In cases where it is allowed by the law.
[129] See para. 46 CJEU decision of 19. 10. 2016 No. C-582/14 (Breyer).
[130] More to the risks of reidentification see Ohm (n 111). More on the legal issues of anonymisation see also WP29 Opinion No 5/2015, on Anonymisation Techniques, online [seen 31. 10. 2022]. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[131] An example from the Czech Republic: A practical example of such data is information from the registers of persons established by Act 304/2013 Sb., on public registers of legal and natural persons. Data from the registers defined by the Act (the Association Register, the Foundation Register, the Register of Institutions, the Register of Unit Owners' Associations, the Commercial Register and the Register of Benefit Corporations) are, on the basis of Section 7 para. 1 of the Act, compulsorily provided by the Ministry of Finance to the extent specified in the act.
[132] Technical barriers to publication are addressed by WP29 in its Opinion No 6/2013, on open data and public sector information ('PSI') reuse, online, p. 10-11 [seen 31. 10. 2022]. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf

accessible individually through a technical measure by filling in a form on a website. Of course, in the latter case it would be theoretically possible to save the registry gradually using an automatic script. But this activity is first of all more demanding and for a layman user of the Internet quite difficult. Secondly, the re-user in such a case would have a considerably more difficult situation to fulfil the conditions imposed on them by GDPR as a data controller.[133] The setting of the way of publication is also important because it can create legitimate expectations among data subjects about how their data is treated (how much it is protected), which is one of the essential aspects in assessing the legitimacy of its possible subsequent use.[134]

Providing personal data in the form of open data is potentially the riskiest way to disclose information, due to the easy technical possibility to use and misuse the data. This fact is highlighted, for example, in the report of the UN Special Rapporteur on the right to privacy.[135] The WP29[136] addressed the issue of the relationship between personal data and PSI (hence open data) in two opinions,[137] which did not rule out the possibility of providing personal data in this way, but strongly warned of the risks that such processing of personal data may entail. In Opinion No 3/2013, which addressed the principle of purpose limitation of processing, WP 29 stated: „*Once personal data are publicly available for reuse, it will be increasingly difficult, if not impossible, to have any form of control on the nature of potential further use, be it for historical, statistical, scientific or other purposes. This is especially the case if the data are available in digital, searchable and machine readable format and have been published on the internet, hence, the selection of the information that will or will not be made publicly available becomes all the more important*."[138] In both opinions, the WP29 refers to the need to carry out a careful impact assessment of the processing of personal data,[139] i.e. what effects the disclosure of personal data may have on data subjects. When assessing the impact, it is useful to consider, for example, whether and what form

[133] More on this topic in part 4.4 of this report.
[134] As will be discussed in more detail in the following section, the main legal ground on which a data controller may rely if they wish to re-use data from public registers is the legitimate interest of the controller within the meaning of Art. 6 para. 1 letter f) GDPR. One of the criteria which intervene in the assessment of the legitimacy of the intended processing is the degree of expectation of the data subject that such processing may take place. For more on this, see e.g. WP29 Opinion No 6/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC [seen 31. 10. 2022]. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[135] Report on Big Data and Open Data from 17 October 2018, No. A/73/438, p. 11 [seen 31. 10. 2022]. Online: https://undocs.org/A/73/438.
[136] WP29 was a working group crated on the bases of Art. 29 directive 95/46/EC and has been transformed to the European Data Protection Board with the applicability of GDPR.
[137] WP29 Opinion No 6/2013, on open data and public sector information ('PSI') reuse and WP29 Opinion No 3/2013, on purpose limitation, online [seen 31. 10. 2022]. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[138] WP29 Opinion No 3/2013, on purpose limitation, p. 49-50.
[139] WP29 Opinion No 6/2013, on open data and public sector information ('PSI') reuse p. 20 and WP29 Opinion No 3/2013, on purpose limitation, p. 50.

of anonymisation or pseudonymisation has taken place over the data as it may act as a technical solution to increase the level of protection of personal data.[140]

The solution to the question of how the publication of information - personal data - should be technically (qualitatively) carried out is surprisingly poorly addressed, both legislatively and doctrinally. If the legislator does not specify the method of disclosure itself, i.e. does not determine a specific norm to be followed (which is very rarely the case), it is necessary to follow the general norms. On the EU level of legal regulation these general norms are Art. 5 OD Directive and relevant provisions of GDPR. A key aspect in assessing the qualitative manner in which PSI - personal data - is to be provided is therefore the purpose of such processing, i.e. the assessment of why the information is provided. As mentioned above, the purpose of the processing is derived from the legal provision on which the obligation to disclose the information is based. The decision on how the disclosure of personal data is technically to be set up must be made on the basis of a consideration of the nature of the personal data provided, the risk that its misuse may pose to data subjects and other factors.[141] In doing so, the principle of minimisation of interference states that the processing should be such that it is the least intrusive on the rights of the data subject in fulfilling the purpose.[142]

The publication of PSI - personal data in the form of open data requires that it is consistent with the purpose for which the information is to be provided. This purpose must be discernible from the statutory formulation of the obligation to provide certain PSI - personal data, or from the formulation of the task of public administration in which such provision is to take place. Therefore, if the legislator explicitly states that the specific PSI - personal data is to be provided as open data, the data provider must comply with this obligation.[143] If the law is not as precise, e.g. it merely states that certain PSI – personal data must be published online, the data provider should evaluate the character of provided data, purpose of the publication of such data that is enshrined in the law, and if possible follow the requirements of Art. 5 OD Directive (or more precisely its national implementation).[144]

---

[140] Borgesius, Gray and van Eechoud (n 104) 2114–2121.
[141] See WP29 Opinion No 3/2013, on purpose limitation, p. 10-12.
[142] A good example from the Czech Republic is access to data from the cadastre. Let us assume that the purpose of this provision is to enable contact with the owner of the property and verify who the owner of the specific property is, and not to enable easy verification of how many properties someone holds. The technical set-up of the described system should thus allow a specific property to be traced via the form, but no longer allow a search based on the property owner's identifier.
[143] E.g. we can expect this situation once the implementing act of OD Directive specifies what precisely what data should contain the high value dataset of "Companies and company ownership".
[144] That is to provide the data "*by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards.*"

To summarise up this section, the data provider can provide PSI – personal data only based on the existence of a legal duty to do so. It is recommended that the law states precisely that the data should be provided in open data quality. But even without this specification, the level of data quality as set by the Art 5 OD Directive is almost at the level of open data. However, it should be stressed that there are limits for the legislator on what data can be legally made public for further re-use. These limits were set by the case law of CJEU. In the case Volker und Markus Schecke and Eifert[145] the court stated that a law requiring too detailed publication of data regarding receivers of agricultural subsidies constituted a breach of right to privacy and right to data protection. Furthermore, in case C-439/19 - Latvijas Republikas Saeima (Points de pénalité) the court categorically denied a possibility of publication for further re-use of PSI concerning special categories of personal data in the meaning of Art. 9 GDPR.[146] These decisions set limits for the legislator of what can be put into law as a duty to publish PSI – personal data.

4.4 Open data re-user as personal data controller

This part addresses legal issues of data re-user as personal data controller, albeit very briefly because this topic is not within the primary focus of this report. Once the PSI - personal data in the form of open data - is published, anyone can take it and process it. However, PSI does not cease to be personal data by its publication. It cannot be taken over and used for any purpose without further ado, as it is still fully subject to the legal framework of personal data protection. An exception to this general rule is where GDPR does not apply, in accordance with Article 2 para. 2 thereof. From an open data perspective, letter c) of this provision is relevant, according to which the processing of personal data carried out by a natural person in the course of a purely personal or household activity.[147] Like all exceptions to the scope of GDPR, processing solely for personal use should be interpreted as strictly as possible. The narrow interpretation of this exception was also confirmed by CJEU in its decisions in Lindqvist Case,[148] where it held that the publication of personal data on a website does not constitute processing for personal or domestic activities, and in Ryneš Case, where it held that the use of a CCTV system to monitor the surroundings of a house does not fall within this exception, despite the fact that only the owner of the property has access to the footage.[149] As a practical example of the use of open data while maintaining the exception of processing personal data solely for personal use, it is possible to mention cases where the interested person downloads the provided information and analyses it to inform themselves or

[145] CJEU decision of 9. 11. 2010, joined cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert.
[146] CJEU decision of 22. 6. 2021, C-439/19 - Latvijas Republikas Saeima (Points de pénalité).
[147] Art. 2 para. 2 c) GDPR.
[148] CJEU decision of 6. 11. 2003, C-101/01 – Lindqvist.
[149] CJEU decision of 11. 12. 2014, C-212/13 - Ryneš.

find out interesting facts, search for connections, etc. However, they may not disseminate this information in any way. This is not a typical use of open data. Given this, the applicability of the exception for open data is very limited.

A common way of dealing with open data is to create various applications and other services that work with the data, which are then offered to end users. If the dataset used contains personal data, the creator of the application is in the position of a data controller, as they determine the purpose of the processing. The purpose may vary significantly depending on the nature of the specific application. Mere 'use of data in an application' cannot serve as a purpose, as the purpose must be sufficiently specific.[150]

Regarding the issue of the data processing purpose, from the open data perspective, Art. 6 para. 4 GDPR may present some interpretative difficulties. Some authors have interpreted it as that its application is necessary even in the case of a takeover of personal data by a new controller.[151] Relative to the case of open data, the user of open data (the creator of the application) would be bound by the purpose (or compatibility with it) for which the data was originally published when determining the purpose of their new processing. However, in our view, this interpretation is not correct, because the purpose limitation principle applies to processing carried out by one and the same controller who established the original purpose for collecting the personal data.[152] In the context of the app creator, the collection of personal data occurs at the moment of download from the data provider's server. We therefore consider that Art. 6 para. 4 GDPR should be read as a provision permitting certain types of processing that are otherwise prohibited by the purpose limitation principle, rather than as a provision further restricting the processing of personal data by third parties.

Once the purpose of the processing of personal data has been determined, the creator of the application working with personal data must provide a legal ground that allows such processing of personal data. Of course, in theory, the data subject's consent is an option,[153] but it will be extremely technically difficult for the data controller to secure it. In practice, therefore, this legal ground is not applicable. From the range of legal grounds listed in Art. 6 para. 1, the only option

---

[150] See, e.g. WP29 Opinion No 3/2013, on purpose limitation.

[151] In Czech, e.g. Michal Nulíček and others, GDPR v otázkách a odpovědích. *Bulletin-advokacie.cz* [online]. Published 3. 11. 2017 [seen 31. 10. 2022]. Online: http://www.bulletin-advokacie.cz/gdpr-v-otazkach-a-odpovedich. It should be added that the same team of authors does not state this opinion in their next publication - Michal Nulíček and others, *GDPR - obecné nařízení o ochraně osobních údajů* (Wolters Kluwer 2017) 140–144.

[152] The same view is very well articulated by Nonnemann, who tries to argue the opposite position in his interpretation, but arrives at the absurd result of the real impossibility of assessing the first two conditions introduced by Art. 6 para. 4 GDPR. See in Czech František Nonnemann, 'Zpracování Veřejně Dostupných Osobních Údajů a GDPR' (2018) 26 Právní rozhledy 167, 169.

[153] See Art 6 para. 1 letter a) GDPR.

available to developers of open data applications with personal data is the legitimate interest of the controller or of a third party within the meaning of letter f) of that provision. A legitimate interest may be the exercise of any right or activity that is generally allowed by law. However, the data controller may rely on this legal ground only if the protection of the rights and interests of the data subject does not take precedence over the declared legitimate interests. Therefore, it can be argued that there is a small institutional (intra-systemic) proportionality test present, which every data controller must assess before starting to process data. It is then the case that the lower the risk of interference with the privacy or other rights and interests of the data subject (whether due to the nature of the personal data or due to their technical security or other aspects), the more likely the data controller may be to be granted this legal ground.[154] It is important to stress that it is not only the fundamental rights and freedoms of the data subject that are at stake, but any interests in general, as is clear from the wording of Art. 6 para. 1, f) GDPR when it states: "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data…".* On the other hand, it is clear from the text of GDPR that European legislator did intend to include a possibility of application of this legal ground to a wide range of various situations, including direct marketing.[155]

Recital 47 GDPPR mentions that the reasonable expectation of the data subject that the intended processing of personal data may take place should be taken into account when assessing the possibility of the application of the legitimate interest of the controller or third parties. For this reason, it is very helpful that in the case of the publication of PSI with personal data, the legislator formulates the intention of their further re-use. In view of the intra-system proportionality test present, the legal title of the processing for the purpose of legitimate interests of the controller constitutes *de iure* an effective protection against misuse of the published personal data. The test of balancing the legitimate interest of the controller against the rights and interests of the data subjects is fundamentally tilted more in favour of the data subjects. However, the legitimate interest can nevertheless serve as a valid legal basis for further processing, especially in the situations when the new data controller creates a new added value to the used content. For example, a mere republication of public database would not survive the test of legitimate interest. However, if the new data controller can find new legal uses for the data which generally add value to what is already public, the balancing test will more likely end up in their favour.

---

[154] For more detailed analysis regarding legal ground of legitimate interest see e.g. WP29 Opinion No 6/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC [seen 31. 10. 2022]. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[155] See recital 47 GDPR.

The final aspect addressed in this chapter is the information duty of the data controller. In the context of open data, Article 14 GDPR is relevant, which sets out what information the controller must provide when personal data are not collected directly from the data subject (which will be the case when working with open data). Paragraph 1 of that Article provides that the controller is obliged to provide the data subject with information on the identity of the controller, the purpose of the processing, the categories of personal data and other information necessary to ensure fair and transparent processing of personal data. According to recital 61 GDPR, this information must then be provided at the time of the collection of the personal data by the controller. Information duty is an essential part of the whole data protection legal framework.[156] Its practical and functional fulfilment is one of the biggest obstacles for effective re-use of PSI with personal data. Due to the large amount of personal data of different data subjects that are processed in the course of such activities by the controller, there is no technically efficient way to comply with this obligation. We are concerned that the method used, whereby the creator of an application using open data with personal data publishes information about the processing of personal data on its website or in the information for its application, is inefficient due to the lack of outreach of this information to data subjects.

GDPR offers two exceptions which might be helpful in this situation. The first one is provision of Art. 11 which reads as follows: "*If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*" However, the data subjects are often fully identified or identifiable if data from relevant registers are published in open data quality. Therefore, this provision will help only in situations, when data provider publishes effectively pseudonymised data, which, however, do not meet the level of security required for their full anonymisation. On the other hand, a number of information sources, such as the commercial register, contain contact details, although often only a physical address. Nevertheless in those cases providing of the information is possible, at least in theory.

The second exception can be found in Art. 14 para. 5 b) which reads: "*Paragraphs 1 to 4 shall not apply where and insofar as the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and*

[156] See e.g. Paul de Hert, Serger Gutwirth. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power. In: Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 77–78. See also Lynskey (n 105) 595; Gabriela Zanfir. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) 245.

safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available."
We can see purposes generally connected with the freedom of speech are expressly mentioned in this exception. And although other purposes are not, the exception is generally applicable on them as well. However, as every exception in GDPR, it must be interpreted as narrowly as possible. Therefore, the question whether there is a "disproportionate effort" must be answered with a great detail and scrutiny. For example, if the dataset contains email addresses of data subjects, it would be hard to argue that sending an information about prepared processing constitutes a disproportionate effort. Thus, application of the second exception is quite questionable.

In our opinion, the best solution would be enacting a law, which would create a register of applications and services which process data taken from public resources, including open data. This register could be run, e.g. by the national data protection authority, or the institution which runs national data portal. If the law expressly states that the register can contain also information regarding existing application, then it is possible to expect data subjects to know about it.[157] Even on the practical level, the main purpose of information duty in GDPR is to be able to know about ongoing processing of personal data. Existence of a central database of open data services would fulfil this purpose and, at the same time, would practically allow data subject to check which applications do use their data, and defend themselves if necessary.

4.5 Chapter outcomes

When it comes to intersection of PSI and personal data, several things must be taken into consideration. Firstly, the application of the OD Directive is limited to the cases, when personal data are provided to the public lawfully. A condition *sine qua non* for that is that there is a legal duty for the data provider to make the data public. However, in some cases, when the national law is in the collision with the international instruments, namely Charter of the Human rights and the EU Law, represented by the EU Charter and GDPR, or with the national constitution, not even a legal duty to make the data public would be sufficient.[158]

Secondly, when there are personal data present in the process of publication of PSI (or more specifically, open data), all parties involved must fulfill duties arising from personal data protection legislation, namely GDPR, because they will be in a positions of data controllers. The

[157] This is because of the legal principle that ignorance of the law does not excuse.
[158] This might be a situation when the publication of data is not proportional.

data provider can publish a dataset that contains personal data only if there is a legal duty to do so. Would there be no such duty, the data provider as a data controller would not have an applicable legal ground (art. 6 para. 1 GDPR) for data processing. This remark is especially true when it comes to publication of personal data in a quality of open data, because the risk of misuse or abuse of such data is higher than in the case of mere online accessibility. The data controller (public sector body providing the data) must also fulfill other duties arising from the GDPR, like to make sure that the data are provided in a way that will not endanger the source database and its integrity and that the data are correct and precise. However, these duties are manageable and achievable.

Thirdly, receivers of personal data that are published in an open data quality are in much more difficult position. They are in a position of a data controller, because the set purpose and means of data processing- These must be lawful and sufficiently specific. Furthermore, the re-users must pass the balancing test, because the legitimate interest (Art. 6, para. 1, letter f)) is the only legal ground that is applicable for this kind of personal data processing. A significant problem consists of the information duty. It is very complicated, and almost impossible, to meaningfully inform data subjects about ongoing data processing in an application that uses personal data. The controller cannot just send every data subject in a database a message and an information published on the webpage of the controller is not sufficient because it will not fulfill the main purpose of information duty. Data subjects must have a chance to know about the ongoing processing so they can defend themselves. However, a mere message on a webpage would be not enough because the data subject would not find that webpage in the first place. Thus, we propose that an alternative solution should be implemented. A central publicly run database of applications and services that use open data datasets with personal data, would solve this problem.

5. Terms of use of open data

When publishing PSI in the form of open data, it is necessary to add to each dataset, in the form of a metadata record, information about the conditions under which the data from the distribution can be used. So-called 'open terms of use', which ensure maximum reusability of content and minimum restrictions beyond the law, are a prerequisite for open data. Thus, the terms of use may include, for example, a license to allow the sharing of content protected by intellectual property rights, information about the presence of personal data or, conversely, information about the legal freedom of the content provided. A technically appropriate way to specify the terms of use of open data may be by placing a hyperlink to the document in the metadata record, where the terms themselves are expressed in a form understandable to the recipient of the data. Typical variations of the terms of use are a link to the standardised Creative Commons licences, a link to a web page with text informing about the open nature of the data provided, and a link to the provider's own terms of use displayed on its website. The main problem with the third group is that they are not standardised in any way and are not machine-readable, which makes it difficult to work with the data afterwards. However, from a legal point of view, it is quite interesting. They are generally used in cases where provided PSI is not protected by any absolute IP rights. There are mainly two types of provisions in the text of the actual terms of use that are of legal interest. Statements of the first type are intended to set out various obligations for the future recipient and re-user of the data. Statements of the second type are intended to exclude or limit liability for future damages that may arise in connection with the use of the data.

5.1 Contract

In a situation where there are during publication of data not involved any IP rights data provider cannot rely on any licence (in *stricto sensu*), because there is no content that could be licensed. However, the data can still be provided under some legally binding conditions. For the legal effect of these conditions, i.e. binding the recipient of the data to a legal obligation to behave or to tolerate something, there must be a contract concluded between the data provider and the data recipient. In the context of open data, it is appropriate to refer to such contractual arrangements as, for example, simple open data contracts, as they do not involve the licensing of any content. It must be a contract because the data provider cannot bind the data recipient to any performance by a unilateral declaration. Thus, in providing open data, it would be necessary to interpret the publication of the data and the publication of the conditions as an offer and the beginning of the use of the data in line with these conditions as an implicit acceptance of the contract. The object of the performance is then the provision of the data on the part of the data provider and the fulfilment of the conditions set out in the attached document on the other.

This part of this research report is necessarily limited by its scope. The question of legality and conditions of a valid contract is subject to the national law and is not harmonised in any way. Therefore, it must be analysed in each jurisdiction separately.[159] From the case law of CJEU, it is clear that a contract governing provision of data is generally possible.[160] Generally, it can be presumed that the following condition should be met regardless of jurisdiction, as it stems from general legal principle of necessity of legal certainty. In order for the terms of use of open data to be understood as an offer to enter into a contract, which could then occur through the use of the data itself, it is necessary that they make it absolutely clear that it is an offer to enter into a contract. This can be achieved, for example, by formulating the text of the terms of use in such a way that it is clear at a first glance that the download and use of the data constitutes a contract with the provider. If the data provider does not comply with this requirement in such a way that it is clear that the terms of use are also an offer to enter into a contract, the contract cannot be concluded and the failure to comply with the provider's requests has no legal consequences. The other way to ensure that a contract is definitely concluded is to make the provision of data conditional on prior registration, which removes the problem of non-addressability of the offer. However, this method cannot be recommended because it contradicts the principle of open data, according to which access to data should be as simple as possible.

In any case, the contract must be within the limits set by the OD Directive. Art. 8 (1) stipulates: "*The re-use of documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective. When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.*" This provision sets a limit to any contract governing the re-use of provided open data. It sets a minimal standard of legal compatibility similarly as other provisions of OD Directive address a minimal standard of technical interoperability with the requirements of "*formats that are open, machine-readable, accessible, findable and re-usable*".[161]

In our opinion, the maximum appropriate level of restriction that can be accepted in order to still be open data is the obligation to give an attribution to the originator of the data. Anything above that level is already, contrary to the principles of open data and to the abovementioned provision of OD Directive.

---

[159] For example, the Czech law generally demands identification of contracting parties. Thus, it is quite complicated to argue that a general contract can be closed in similar way as Creative Commons licences, which have in the Czech law specific regulation that expressly allows this licensing practice (but is applicable only when there is present IP protected content).
[160] See CJEU decision of 15. 1. 2015, No. C-30/14 (Ryanair Ltd v PR Aviation BV).
[161] See Art. 5 (1) OD Directive.

5.2 Open Licences

As results from the findings of chapter 3 of this report, in most cases there is no need to consider licensing in any way when providing open data because of the legal freedom of plain data and the fact, that the data provider can license *in stricto sensu* only content protected with an IP right. Furthermore, the easiest way for PSI publication would be a case when we can apply statutory exceptions or limitations. Unfortunately, neither the directive 2000/29/EC nor the directive 96/9/EC offer such exceptions and limitation, that would be applicable for re-use of open data.[162] A possible solution, at least for some re-use applications, offers directive 2019/790 (DSM Directive).[163] Articles 3 and 4 of DSM Directive introduced exceptions for text and data mining, which must the member states mandatorily introduce into their legal frameworks. Unfortunately, neither these exceptions are sufficient for effective and complex re-use of PSI.[164] Therefore, licensing is the only viable option for securing a possibility of a re-use of PSI protected with IP rights.

There are three situations in which content licensing is possible and necessary for open data. A necessary prerequisite for all three is that the data provider is entitled to grant a licence (or sub-licence). If this were not the case, and a licence were nevertheless granted, this would be acting contrary to the *nemo plus iuris* legal principle.[165] A licence may be granted in the following situations: i) the copyright work is part of the distribution of the dataset provided; ii) the structure of the database is copyrighted as an original database; iii) the content of the database to be provided is protected by a special right of the acquirer. In addition, these three options may be combined.

A suitable tool for licensing content protected by intellectual property rights is the so-called "public licences". The aim of public licences is to ensure that the licensed content is open, i.e. that anyone can freely use the licensed work for any purpose, subject at most to attribution and openness. The public nature of the licence is determined by its regulated contracting process. This takes the form of a non-addressed public offer to enter into a licence agreement, which occurs implicitly at the beginning of the use of the work, subject to the terms and conditions set out by the licensor through publicly available licence terms. This implies that no real interaction between the licensor and the licensee is necessary and that there is no prior knowledge or limitation on the range of persons who may enter into the contract. It also means that if the licensee breaches the

[162] More on this argumentation see in the context of database rights Jakub Míšek, 'Open Data, Open Api and Database Rights' [2019] Jusletter IT 1.
[163] 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
[164] For more context see e.g. Jakub Míšek, 'Exception for Text and Data Mining for the Purposes of Scientific Research in the Context of Libraries and Repositories' [2020] The Grey Journal.
[165] The principle states that no one can transfer more rights than they have themselves.

terms of the licence, the licence is lost and further use of the work is then unlawful. We can define a public licence with a list of the following minimum defining characteristics:

- non-addressability and irrevocability,
- automatic implied acquisition of the licence by use of the work,
- non-exclusivity,
- territorial, temporal, quantitative and material unlimitedness,
- the right to share,
- royalty-free,
- minimisation of the licensor's liability and warranties,
- the condition of attribution.

There are a number of public licences that data providers can use to license open data.[166] A good example of a public licence that is recommended by the general open data community is the Creative Commons licences, specifically the CC BY 4.0 and CC0 1.0 licences. Therefore, in this report we focus on these licences as well. Creative Commons licences are made up of three layers: i) the legal text; ii) a human-readable version summarizing the rights and obligations under the license (the "deed"); and iii) a machine-readable layer that allows automated evaluation of which license with which terms is being used.[167] One of the reasons why Creative Commons licences are recommended as standardized licences for open data publishing is precisely because their machine-readability enables automated evaluation of licences within open data catalogues and makes it easier for data recipients to work with them. The second advantage is their international familiarity and availability. Together these two reasons help significantly to legal interoperability between different jurisdictions and different data providers. Open data providers may choose to use other (or their own) licences. However, this will result in a loss of machine readability and, if the license is written in not so common language as for example Czech or Hungarian, to a deterioration of the ability to use the data abroad. Therefore, we cannot recommend this approach and it is highly recommended that data providers use standardised public licences.

The CC BY 4.0 (Attribution 4.0 International) licence is the most open license in the Creative Commons family of licences. It can be used for licensing copyrighted works. This license is applicable to both copyrighted works and the *sui generis database rights* allows the receiver of the content to share, modify and use the protected content for any purpose. The only conditions for

[166] See e.g. Primavera De Filippi and Lionel Maurel, 'The Paradoxes of Open Data and How to Get Rid of It? Analysing the Interplay between Open Data and Sui-Generis Rights on Databases' [2014] International Journal of Law and Information Technology <http://ijlit.oxfordjournals.org/content/early/2014/10/16/ijlit.eau008>
[167] See https://creativecommons.org/.

use of the work under the CC BY 4.0 licence is to give an attribution. This means that that the origin of the work must be indicated, i.e., its title (or other clear identification), the author, and further there must be present a reference to the text of the license.[168]

The CC0 1.0 license is not a contract, but a unilateral waiver of absolute rights to the protected content.[169] In view of this, it cannot be applied as waiver in jurisdictions, where waiver of a copyright is excluded by a law. If the CC0 licence is wrongly used by the licensor to license the copyright work, Article 3 of the CC0 licence will apply (the so-called "Public License Fallback"), according to which in cases where national law does not allow the waiver of an absolute right, CC0 is to be interpreted as granting the most open licence (e.g. CC BY). However, the CC0 license can be used to waive the *sui generis* database right and in such a case, the *sui generis* right is irrevocably terminated. Because CC0 is a unilateral act, it can be used also as an information tool to communicate to the data receivers, that the content is not protected by intellectual property rights in any way. However, this approach may create some level of legal uncertainty and therefore it cannot be recommended without a reservation.

5.3 Providing information about the dataset

An important duty of a open data provider is to maximise legal certainty od the data recipient so the provided open data can be re-used as easily as possible. A good way of fulfilling this duty is to prepare transparent and understandable "*Terms of use*" of the provided dataset. The main purpose of Terms of use is therefore to provide information about the legal status of published open data. However, in case there is present a legally protected content in the dataset, the Terms of use should deal with this problem as well. Technically, a good way how to communicate Terms of use to the data recipient is adding them to the metadata record of provided open data release.

The terms of use may include licences that allow for the use of the content of the dataset. As the previous chapters of this report have shown, during the publication of open data, it is possible to encounter, albeit exceptionally, copyright works as part of the open data content, the copyrighted database (its structure or way of selection of the content) and *sui generis* database rights of the database maker. In cases where there is no IP law protected content present in the dataset, it is also advisable to inform the recipient of the data of this fact in order to ensure his legal certainty. In licensing, it is absolutely essential to ensure that open data providers apply licenses only where possible and necessary and that the licensed content is clearly identified. Granting a single "global" licence for the entire dataset release is inadequate and confusing because it does not identify the

[168] See online: https://creativecommons.org/licenses/by/4.0/.
[169] See online: https://creativecommons.org/share-your-work/public-domain/cc0/

exact content to which the licence applies. This reduces the legal certainty of the recipient of the data. If in a particular case it is not possible to identify which content is specifically covered by the licence, the consequence would probably be that the licence would be void for ambiguity. A suitable way to include licenses in the metadata structure describing the distribution of the dataset is to split the 'terms of use' section into three entries according to the intellectual property rights that may be involved in the publication of open data.

In addition to these intellectual property rights, personal data may also be present in the dataset. Therefore, the terms of use should also inform about their presence or absence, thus adding a fourth entry in the metadata record in the 'terms of use' section. Each of these four entries makes it possible to clearly identify whether or not the listed protected content is present, or under which licence its re-use is allowed.

A proper construction of Terms of use is described by the licensing scheme in the Part II of this research report (see Figure 2).

5.4 Chapter outcomes

An essential part of providing open data is to specify the terms of use. Their primary purpose is to inform the recipient of the data about the legal status of the dataset provided. However, the nature of the terms of use will vary depending on the type of content present in the dataset provided. If the dataset includes content protected by copyright (whether the content itself or a copyrighted database) or sui generis database rights, licensing of such content is necessary to properly allow the re-use of such data. In this case, the terms of use will be constituted by a licence agreement. An appropriate solution is to use public licenses such as Creative Commons CC BY 4.0 or a CC0 waiver. The great advantage of this solution is its wide international recognition and applicability.

If the open data provided does not contain any content protected by intellectual property rights, it is still possible to make the provision and re-use of the data subject to a data disclosure agreement. In this contract, the recipient commits to comply with the conditions set by the data provider. This solution raises three main problems. The first is primarily legal. It relates to the fact that the conditions that need to be fulfilled in order for a contract so constructed, directed to an indefinite number and range of recipients, to be validly concluded and therefore legally enforceable will vary from jurisdiction to jurisdiction. A possible solution to this problem is to introduce prior registration before the provision of data. However, this is contrary to the principles of open data as such. The second problem is that the terms of setting up such a contract are limited by the requirements of the OD Directive and, in particular, must not restrict in any way the further use of the data provided beyond the scope of the OD Directive. The third problem relates to legal interoperability and its technical implementation. The custom contract and the

custom terms of use will not be standardised. They will probably not even be machine-readable and automatically processable. This makes the automatic re-use of the data provided much more complicated. In view of these problems, we cannot recommend the provision of open data on the basis of custom ad hoc contracts.

The main purpose of the terms of use is to inform the recipient of the data about the possible legal obstacles that may be associated with the provided content and, where appropriate, to provide solutions to them (licenses for content protected by intellectual property rights). The terms of use must therefore include a specification of what specific IP rights are associated with the data provided and how these rights are licensed. If the data provided contains personal data, it is also necessary to inform the recipient of the data of this fact so that they know that by processing it they will be in the position of a data controller. Finally, if the data provided is really just plain data without any accompanying legal protection, it is again advisable to inform the recipient of the data of this fact to ensure their legal certainty. Guidelines for the creation of the terms of use and a flowchart thereof are contained in Part II of this report.

Part II: Guidelines and a licensing scheme

The following guideline summarises the legal analysis presented in the Part I of this report in a form of a checklist. To make further use of the data at European level a success, the re-user must have a high level of legal certainty that there are not any legal obstacles for further use of the data. This issue, however, must be properly addressed by the data providers. The following checklist should serve as a tool that helps data providers to be sure that they have not neglected any important issue during the process of data publication.

Step 1: Access to the data

- Check regulation of access of information
  - What laws do govern access and publication of information?
  - How was Open Data Directive implemented into the national legal order?
  - Is there any specific act, that covers publication of datasets of public registers of companies and other legal entities?
    - If yes, this act will generally be applicable.
    - If no, a general freedom of access to information or similar act will be applicable.
- Does public sector body have a legal duty to publish the data?
  - Are the data part of HVD in accordance with OD Directive?
  - Is there a national regulation, that constitutes the duty to publish the data?
  - How precisely is the duty stipulated? (E.g. is it general like "Data from the register", or is it more specific enumeration of data categories?)
- Does public sector body have a discretion to publish data?
  - Can the public sector body generally publish data without a specific legal obligation to do so?
    - This will apply in cases, when there is not a duty to publish specific datasets, or in cases, where there is such a duty, but the public sector body would like to publish more, than the duty prescribes.

Step 2: Intellectual property rights protection

- For proper licensing scheme it is necessary to identify protected content and make sure that the data provider can license it.
- Each dataset can be subject to several intellectual property rights.
- Are plain data in your jurisdiction protected by any kind of intellectual property or property rights?

    - If no (which will probably be the most cases), this will not constitute an obstacle for publication and re-use of data
    - If yes, it is important to identify, whether the data provider is owner of the data (or whether they exercise the rights to the content)
        - If yes, the content can be provided and licensed under public licence (preferably CC0 or CC BY 4.0).
        - If no, the content cannot be provided.
- Does the dataset contain copyrighted content?

  E.g. there are copyrighted literal or artistic works in the dataset, or the dataset is a map
    - If no (which will probably be the most cases), this will not constitute an obstacle for publication and re-use of data
    - If yes, it is important to identify, whether the data provider can exercise the rights to the content
        - If yes, the content can be provided and licensed under public licence (preferably CC BY 4.0, or CC0 if your jurisdiction allows to waive the copyright).
        - If no, the content cannot be provided.
- Is the database protected by copyright itself?

  I.e., are there fulfilled the requirements that a) it is the author's intellectual creation, and b) the selection of the elements and their arrangement must be the result of creative activity?
    - If no (which will probably be the most cases), this will not constitute an obstacle for publication and re-use of data
    - If yes, it is important to identify, whether the data provider can exercise the rights to the content (which will probably be most of the cases)

      In some cases, it is possible to provide dataset without licensing the copyrighted database. It will depend on, whether the export of the database directly follows its structure and selection of elements. If not, then the exported dataset will not infringe the copyright.
        - If yes, the database can be provided and licensed under public licence (preferably CC BY 4.0, or CC0 if your jurisdiction allows to waive the copyright).
        - If no, the content cannot be provided.
- Is the database protected by *sui generis* right?

I.e. there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents

This step is essential because *sui generis* database right directly affects the provided content.

- If no, this will not constitute an obstacle for publication and re-use of data
- If yes, it is important to identify, whether the data provider is maker of the database (which will be most of the cases) or whether they can exercise the rights to the content
  - If yes, the database can be provided and must be licensed for further re-use, preferably under public licence (CC BY 4.0, or CC0 if your jurisdiction allows to waive the sui generis database right).
  - If no, the content cannot be provided.

Step 3: Personal data protection

- If the dataset contains personal data, it is essential that they are provided only in accordance with personal data protection law (primarily GDPR) and that the data re-users are properly informed about the presence of personal data, so they can effectively comply with their duties as data controllers.
- Does the dataset contain personal data?
  - If no, this will not constitute an obstacle for publication and re-use of data
  - If yes, is there a legal duty to provide such data as open data?
    - If yes, the dataset can be provided
    - If no, the content cannot be provided.
- The data provider can lower the risk of misuse of the provided personal data by conditioning their provision with a conclusion of a contract, which would bind the re-user to use the data in a certain foreseeable way. E.g. the data provider can limit purposes of re-use. However, it must be noted, that because of such further conditions, it would not possible to identify such provided information as open data.
- If the personal data cannot be provided, the data provider still can conduct a thorough anonymisation, which would render personal data non-personal. It is important to note, that the anonymisation has to be prepared thoroughly and diligently because there is a higher risk of de-anonymisation, once the dataset is publicly and freely available.

Step 4: Preparation of Terms of use

- Once the data provider identifies legal obstacles that could prevent the publication or re-use of the data, it is essential to communicate results of their findings to the data re-user.
- Terms of use should contain information about any content that is subjected to any kind of information protection, whether it is copyright or personal data protection. It also must contain any solution which overcomes such protection, such as licences.
- Terms of use should be easily accessible and preferably part of the metadata of the dataset.
- For the sake of legal certainty, it is advisable to precisely identify what intellectual property rights are present in the specific instances of provided dataset and how precisely they are licensed.
    - E.g. the data provider can decide, that copyrighted content is licensed with CC BY 4.0 public licence and at the same tam, that *sui generis* database right is waived with CC0.
- If the dataset contains personal data, the terms of use must contain this information. It is not possible to licence personal data. The re-user will have to fulfil all the duties arising from GDPR and national laws of data protection.
- If the dataset does not contain any protected content, the terms of use should state this information for the sake of legal certainty.
- The data provider can provide the data under other conditions and after a conclusion of a contract. However, imposing of such additional obligations for data re-use would lead to a situation, in which the provided content would no longer be truly open data.
    - Furthermore, should the data provider decide to do so, firstly they must ensure, how the national law allows for and what are conditions for a valid conclusion of a contract online.

Graphical version of the licensing (Terms of use) scheme (flowchart)

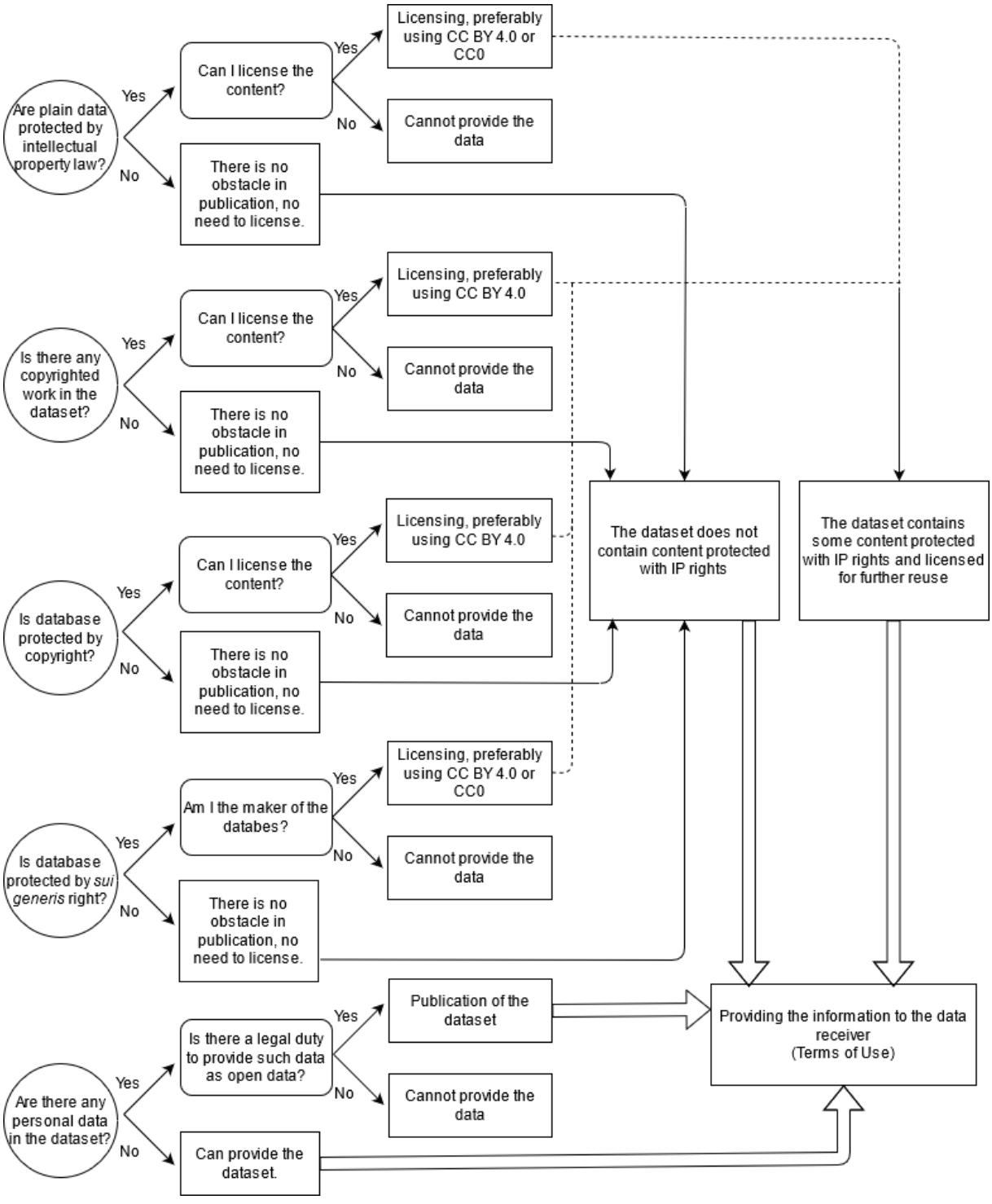

Figure 2 Terms of Use Scheme

List of selected resources

Adriaans P, 'Information' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Metaphysics Research Lab, Stanford University 2013) <https://plato.stanford.edu/archives/fall2013/entries/information/> accessed 30 June 2019

Boerding A and others, 'Data Ownership - A Property Rights Approach from a European Perspective' (2018) 11 Journal of Civil Law Studies 323

Borgesius FZ, Gray J and van Eechoud M, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework' (2015) 30 Berkeley Technology Law Journal 2073

Buckland MK, 'Information as a Thing' (1991) 42 Journal of the American Society for Information Science and Technology 351

Burkert H, 'Public Sector Information: Towards a More Comprehensive Approach in Information Law' [1992] Journal of Law and Information Science 47

Bygrave LA, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35 Oxford Journal of Legal Studies 91

Claes E, Duff A and Gutwirth S (eds), *Privacy and the Criminal Law* (Intersentia 2006)

Eechoud MV and Janssen K, 'Rights of Access to Public Sector Information' (2013) 6 Masaryk University Journal of Law and Technology 471

Fadler M and Legner C, 'Who Owns Data in the Enterprise? Rethinking Data Ownership in Times of Big Data and Analytics' [2020] Proceedings of the European Conference on Information Systems (ECIS) 1

Filippi PD and Maurel L, 'The Paradoxes of Open Data and How to Get Rid of It? Analysing the Interplay between Open Data and Sui-Generis Rights on Databases' [2014] International Journal of Law and Information Technology <http://ijlit.oxfordjournals.org/content/early/2014/10/16/ijlit.eau008> accessed 4 December 2014

Floridi L, *Information: A Very Short Introduction* (Oxford University Press 2010)

Geiger C, 'Promoting Creativity through Copyright Limitations: Reflections on the Concept of Exclusivity in Copyright Law' (2009) 12 Vanderbilt Journal of Entertainment and Technology Law 515

Gellert R, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 3

——, ‘Understanding Data Protection as Risk Regulation’ (2015) 18 Journal of Internet Law 3

Gutwirth S, Leenes R and De Hert P (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

Hood C, Rothstein H and Baldwin R, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001)

Hooghiemstra T, ‘Informational Self-Determination, Digital Health and New Features of Data Protection’ (2019) 5 European Data Protection Law Review 160

Hugenholtz PB, ‘Directive 96/9/EC’ in Thomas Dreier and P Bernt Hugenholtz (eds), *Concise European copyright law* (Second edition, Kluwer Law International 2016) <https://media.wolterskluwer.com/pdfs/SampleChaptersPDF/6651.pdf>

Hugenholtz PB and Quintais JP, ‘Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?’ (2021) 52 International Review of Intellectual Property and Competition Law 1190

Lee M, Almirall E and Wareham J, ‘Open Data and Civic Apps: First-Generation Failures, Second-Generation Improvements’ (2016) 59 Communications of the ACM 82

Lillà Montagnani M and von Appen A, ‘IP and Data (Ownership) in the New European Strategy on Data’ (2021) 43 European Intellectual Property Review 156

Lynskey O, ‘Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the Eu Legal Order’ (2014) 63 International & Comparative Law Quarterly 569

Míšek J, ‘Open Data, Open Api and Database Rights’ [2019] Jusletter IT 1

——, ‘Exception for Text and Data Mining for the Purposes of Scientific Research in the Context of Libraries and Repositories’ [2020] The Grey Journal <https://is.muni.cz/auth/publication/1608958/cs/Exception-for-Text-and-Data-Mining-for-the-Purposes-of-Scientific-Research-in-the-Context-of-Libraries-and-Repositories/Misek> accessed 28 November 2022

Morozov E, *To Save Everything, Click Here: The Folly of Technological Solutionism* (PublicAffairs 2013)

Nonnemann F, ‘Zpracování Veřejně Dostupných Osobních Údajů a GDPR’ (2018) 26 Právní rozhledy 167

Nulíček M and others, *GDPR - obecné nařízení o ochraně osobních údajů* (Wolters Kluwer 2017)

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701

Peixoto T, 'The Uncertain Relationship between Open Data and Accountability: A Response to Yu and Robinson's the New Ambiguity of Open Government' [2012] UCLA Law Review Discourse 200

Ruijer E and Martinius E, 'Researching the Democratic Impact of Open Government Data: A Systematic Literature Review' (2017) 22 Information Polity: The International Journal of Government & Democracy in the Information Age 233

Safarov I, Meijer A and Grimmelikhuijsen S, 'Utilization of Open Government Data: A Systematic Literature Review of Types, Conditions, Effects and Users' (2017) 22 Information Polity: The International Journal of Government & Democracy in the Information Age 1

Santos CD, 'On Privacy and Personal Data Protection as Regards Re-Use of Public Sector Information (PSI)' (2013) 6 Masaryk University Journal of Law and Technology 337

Schwartz PM and Solove DJ, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814

Sganga C, 'The Notion of "Work" in EU Copyright Law after Levola Hengelo: One Answer Given, Three Question Marks Ahead' (2019) 41 European Intellectual Property Review 415

Thorhildur J, Avital M and Bjørn-Andersen N, 'Generating Value from Open Government Data', *International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design* (2013)

Yu H and Robinson DG, 'The New Ambiguity of Open Government' (2011) 59 UCLA Law Review Discourse 178

Authors:

JUDr. MgA. Jakub Míšek, Ph.D.

JUDr. Radim Charvát, Ph.D., LL.M.

doc. JUDr. Matěj Myška, Ph.D.

Masaryk University

Žerotínovo nám. 617/9, 601 77 Brno, Czechia

Brno 2022