Understanding some of the open data challenges to data protection in the developing European legal framework

Tihomir Katulić, Anamarija Musa
University of Zagreb
Faculty of Law
Trg Republike Hrvatske 14, Zagreb
{tihomir.katulic, anamarija.musa}@pravo.unizg.hr

Darja Lončar
Rimac Group
Zagreb
darja.loncar@rimac-automobili.com

Abstract. *According to the EU Charter of Fundamental Rights, both the right to privacy and the right to the protection of personal information are different, emancipated rights that are complementary to one another. The high level of data protection was further improved by the General Data Protection Regulation. Open data is information that may be used for commercial or non-commercial purposes and is made accessible to the public in an open and machine-readable manner. It is anticipated that open data would increase public sector openness while also fostering the (data) economy and data-driven innovations, particularly with regard to the IT services sector and SMEs. The Open Data Directive has established rules for the release of open data and the re-use of public sector information in the EU. The new European data strategy from 2020 has underlined the necessity for open data, even outside of the data owned by the public sector. According to this strategy, the EU's single market for data will be strengthened by using more open data. Consequently, the EU has adopted the new Data Governance Act as a cross-sectoral instrument that tries to increase data accessibility by regulating the reuse of protected data held by public sector, promoting the sharing of data for altruistic purposes and regulating data intermediaries as a novel approach to fostering open data economy.*[1]

Keywords. Open data, data protection, DGA, GDPR

1 Introduction

This paper contains a brief overview of the respective EU data protection and open data legislation, i.e., the notions of data protection and open data as understood in the EU law. The central part of the paper will deal with the intersection between data protection and open data by analyzing selected aspects which seem to be especially relevant for balancing between data protection and open data.

Legislative activities of the European Union (EU) have long ago established a global standard of data protection and privacy legal framework. Both the right to protection of personal data and right to privacy are distinctive, emancipated (Gonzalez Fuster, 2014) yet supplemental and parallel fundamental rights of individuals as regulated by the EU Charter of Fundamental Rights of the European Union. The 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; GDPR) which became applicable in 2018 has additionally raised this level of data protection adopting a number of mechanisms aimed at ensuring an adequate level of compliance in relation to perceived risk to potential data breaches from the perspective of data controllers and processors (Katulić, Vojković 2016), although even then there were opinions that some of its finally agreed upon provisions, like the layered approach to data breach reporting, have somewhat blunted the efficacy in general prevention (Papakonstantinou, De Hert 2016).

The Regulation has also explicitly regulated the data subject data protection rights, including the data portability right and laying out the rules for restriction of these rights while respecting the essence of the fundamental rights and freedoms when necessary (Art. 12 to 23 of the GDPR).

2 Open Data in the EU legal framework

For the past twenty years public authorities have been increasingly pressured to open their data for public use,

[1] The paper is a result of the TODO project based on received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 857592.

from the users' communities (NGOs, SMEs, etc.) but also from the highest political levels (e.g., endorsement of the Open Data Charter by G8, OGP etc.).

Open data is data which is available to the public in the machine-readable format for commercial or non-commercial (re)use (Van Loenen, Zevenbergen, de Jong, 2012). It is expected that open data will improve transparency of the public sector but also help boost the (data) economy, data-driven innovations, especially with respect to IT services industry and SMEs (Wessels 2012). In the EU, the issue of open data and the re-use of public sector information has been regulated by the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive).

The new European strategy for data from 2020 has additionally emphasized the need for open data, even beyond the data held by public sector. Within this strategy the open data is perceived extremely important for strengthening the EU single market for data. The new 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 or DGA) complements the Open Data Directive but also goes beyond it. The Data Governance Act was proposed by the European Commission in 2020 and adopted by the European Parliament in 2022. The Act (EU) 2022/868 will apply from September 2023.

It extends the scope of openness of data held by public sector by imposing obligation of openness, under certain conditions, also to data which are subject to rights of others, including on the grounds of protection of personal data. The second important piece of legislation within the European strategy for data is the Proposal for a regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). The Proposal of Data Act extends the obligation of data openness to data held by private sector as well, thus substantially changing the paradigm of open data in EU.

The GDPR, as its full name suggests, is not only about protecting personal data but also about the free flow of data in the EU market. Similarly, Open Data Directive, Data Governance Act and Proposal of Data Act emphasize the necessity to comply with the GDPR and respect the right to protection of personal data. Nevertheless, it seems that data protection and open data are on the opposite sides of the openness/data protection legal debate. The question put forward is to what extent these opposing concepts can be balanced. What are the challenges to protection of personal data from the open data legislation, in particular as of the new European strategy of data, and vice versa? Is it possible to achieve adequate openness of data as required by the EU open data legislation, while at the same time preserving the right to protection of personal data as required by the EU data protection standards?

The open data and personal data protection come into conflict most often in cases when the users of open data, such as civil society organizations combating tax fraud and corruption or business organizations creating new content based on different databases, require datasets containing personal data (names) of politicians and civil servants or receivers of public funding such as subsidies, or demand full access to company registers in the open data format and similar. In these cases two issues have to be considered.

Firstly, whether the personal data is public information which could be accessible to public in any form. The question relates to the traditional balancing between transparency for the sake of accountability and efficiency of public organizations, and personal data protection with the purpose to protect privacy. The second issue concerns the measure to which this information, if public at all, should be made available in open data format to be further processed and disseminated outside the public bodies and their public functions for the purpose for which it is not initially collected. Usually, these issues are discussed and thought through in each particular case, depending on the wider context in which data is requested.

Any type of personal data processing, including re-use of personal data within the concept of open data, must rely on at least one of the legal bases from Article 6 GDPR (and Article 9 in case of special categories of personal data) to be lawful. When processing is based on (national) law imposing obligation to open data or public interest (Article 6.1.c) and e)), the certain quality of law is required. To what extant are these GDPR requirements of lawfulness recognized by the EU open data legislation? The Data Governance Act also introduces the concept of “data altruism” where individuals can consent to re-use of their personal data for altruistic purposes (e.g., in health, mobility). To what extent is consent approach from the Data Governance Act similar to the one from the GDPR? Also, we shall tackle to what extent are data protection principles affected with the open data concept.

Another line of argument and analysis concerns the advent of machine learning technologies, colloquially referred to as AI (Artificial Intelligence). The development and use of these technologies relies heavily on the use of personal data, and open data is seen as a supporting and contributing effort to further development of these critical systems for future information society products and services (Grafenstein, 2022).

At the same time, as the legal foundation of the European system of human rights, the Charter of Fundamental Rights incorporates substantial checks and constraints on the effect and aim of future EU AI regulation. Whenever and however this law is enacted, it must comply with and contain existing European legal standards pertaining to persons' fundamental rights in the EU. The European Commission's ethical guidelines and the opinions of data protection authorities and institutions such as the EDPS and the

EDPB lay out ethical standards based on recognized fundamental rights that future AI systems must follow in order to be trusted and secure from the standpoint of enacted principles of personal data protection.

The interplay between the data protection and open data, especially as regulated within the new European strategy for data, is very new. Against this background and in conclusion, the authors would like to identify problems and raise questions which seem to us especially relevant in balancing data protection and open data, acknowledging the scope of the problem and inviting further study and research.

3 Digital Governance Act

After several years in development, the European Commission released its new open data strategy document, the European Data Strategy in 2020, in which it detailed its vision for the building of a European data economy over the next decade.

Main goal of the strategy is to promote use of available data in all economic sectors as this is vital to the development of digital economy. Currently there are plenty of arguments why the EU market has not been able to leverage the available data in order to develop new information society products and services and previous research has identified numerous factors which have had a stifling influence on the development of information economy, such as general lack of data availability, market power imbalances, insufficient governance structures and technical infrastructure or the lack of adequate tools to enable data subjects (consumers, users of services, general public) to efficiently exercise their rights related to data sharing, such as the GDPR Article 20 Data Portability Right (Gellert, Graef 2021).

The Open Data Directive governs the re-use of publicly available information maintained by the public sector. The public sector, on the other hand, maintains huge volumes of protected data (e.g., personal data and commercially secret data) that cannot be re-used as open data but could be re-used under special EU or national legislation. A wealth of knowledge can be derived from such data without jeopardizing its protected status, and the Data Governance Act (DGA) includes guidelines and protections to facilitate such re-use if permitted by other laws.

The DGA is an important part of a the wider legislative effort the EU has undertaken to create rules for future digitalization, data economy, artificial intelligence, and other major policy goals sometimes referred to as digital sovereignty.

Because artificial intelligence research is reliant on having access to enormous pools of data, data is a critical component in this framework. Similarly, virtually all new information society services, digital goods, and apps rely on data availability for at least some of their performance. Lastly, the availability of enormous volumes of data is becoming increasingly important in scientific study in general.

The DGA's objectives are substantial. The major purpose is to promote the European data economy and to strengthen the EU's digital single market as it tries to play catch-up with United States and SE Asia (Voss 2020), birthplaces of most of today's innovative services and platforms. With this in mind, and with hope to empower the entrepreneurial culture of the European market, small and medium-sized firms (SMEs) and start-ups are given special attention. These entities especially benefit from planned data reuse and data sharing which provides new material for innovation in artificial intelligence and digital applications (Ruohonen, Mickelsson 2023).

Scientific research is also an essential component of the goals of the Digital Governance Act. Data is regarded as essential for combating a range of current economic and societal issues, also helping with adapting to and preventing climate change, supporting the green transition, as well as enhancing energy infrastructure, healthcare, and financial services. These objectives are to be met in specific "European style" of approaching data and the data economy, following that any proposed policy should ensure a fair and legal framework for reuse of data, especially from the perspective of data protection principles (Ruohonen, Mickelsson 2023).

The DGA itself is divided into eight chapters, from introductory provisions and definitions of key concepts and terms to provisions regarding the re-use of certain categories of protected data held by public sector bodies, requirements to data sharing services, data altruism, oversight of competent authorities over the application of the Regulation and establishment of the European Data Innovation Board.

4 From GDPR to DGA

The DGA defines the concept of data altruism, requiring Member States of the EU to adopt a horizontal regulation for the re-use of specific types of protected data stored by public sector organizations, the provision of data intermediation services and data altruistic services.

Data altruism is defined in the Article 2 of the Regulation as "...voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law".

These provisions, according to Article 2 of the DGA, would relate to sectors such as healthcare, fighting climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the

provision of public services, public policy making or scientific research purposes in the general interest (Article 2 of the DGA).

Organizations that make relevant data available based on data altruism will be allowed to register as "data altruism organizations recognized in the Union" (DGA Art. 19 and 20). These institutions must be non-profit, fulfill transparency criteria, and provide particular protections to protect the rights and interests of individuals and businesses who share their data. Moreover, they must comply with the rulebook (prepared by the European Commission – the Commission will draft the rulebook in close collaboration with data altruistic organizations and other relevant parties at least 18 months after it becomes effective), which will include information requirements, technical and security requirements, communication roadmaps, and suggestions on interoperability standards (Recitals 46, 58 and Article 22 of the DGA). The organizations will be allowed to use the common symbol created for this purpose, and they will have the option of being included in the public register of data-altruism organizations. The Commission will create an EU-wide register of recognized data/altruism organizations for information purposes.

While referring to concepts and definitions already defined in the General Data Protection Regulation, such as personal data, data subjects, consent, and data processing (Article 4 of the GDPR), DGA also defines or updates definitions of specific terms and concepts such as re-use of data, data holders, data users, data sharing and data intermediation services in a way resembling the similar provisions in the GDPR (Papakonstantinou, De Hert 2021). As Papakonstantinou and de Hert already observed in 2021, the DGA constitutes a system remarkably similar to the one established by GDPR building on the concepts dating into the 1990s and Data Protection Directive, or even earlier to CoE Convention 108.

The DGA defines re-use as use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks. Data holders are defined as legal persons - including public sector bodies and international organizations - or a natural person who is not a data subject with respect to the specific data in question, which have the right to grant access to or to share certain personal data or non-personal data in line with the applicable EU or Member State law. Data users are understood as natural or legal persons who have lawful access to personal or non-personal data and have the right to use that data for commercial or non-commercial purposes in accordance with applicable law (in case of personal data, the GDPR).

The DGA further develops the concept of data sharing as provisioning of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data. The provisioning is based on voluntary agreements or Union or national law and can be facilitated directly or indirectly through an intermediary. The data might be available free of charge or be available under various open or commercial licenses. Many businesses are concerned that sharing their data would result in a loss of competitive advantage as well as the danger of potential abuse and litigation. The DGA establishes a set of rules for providers of data intermediation services (such as data markets) to follow in order to serve as trustworthy organizers of data sharing or pooling inside the shared European data spaces. The framework offers a new approach to the data-handling methods of Big Tech platforms, which have significant market influence due to their ownership over massive volumes of data.

In practice, data intermediates will serve as impartial third parties connecting individuals and data holders on one side with data users on the other. They will be unable to commercialize the data by selling it to another business or developing their own product based on it. Intermediaries will be subject to stringent standards in order to maintain their impartiality and avoid conflicts of interest. In reality, this implies that the data intermediation service and any additional services supplied must be structurally isolated (i.e. they must be legally separated). This innovative approach suggests a strategy based on the neutrality and openness of data intermediaries, while placing consumers and businesses in control of their data, in order to promote confidence in data sharing.

The DGA defines data intermediary services as services that establish commercial relationships between an undetermined number of data subjects and data holders one hand, and similarly an undetermined number of data user on the other hand. Intermediation services as defined by the DGA do not include services such as those that focus on intermediation of copyright protected content, services that are offered by public sector bodies that do not aim to establish commercial relationships, services exclusively used by one data holder or used by multiple legal persons in a closed group or services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of such data to data users (Article 2.11).

The similarities to the GDPR do not end with definitions of key concepts. DGA introduces principles of provisioning data sharing services in Article 11 such as transparency (Article 11.4 – 11.6), non-discrimination (11.6) and fair competition (11.6), special rights for individuals that want to participate in data altruism, such as regulation of the European data altruism consent form (Article 25), duty of data altruism organizations to inform data subjects on information pertinent to processing, such as the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which

personal data is to be processed, and for which it permits the processing of their data by a data user (Article 21.1.a) etc. DGA also establishes a new permanent institution, the European Data Innovation Board (Article 29).

Article 3 of the DGA defines the types of data that can be reused. DGA applies to data kept by public sector organizations that are protected by commercial secrecy, statistical confidentiality, intellectual property protection, and personal data protection. As a result, personal data kept by public sector organizations is covered, and thus the GDPR also applies. This provision also recognizes certain exceptions, excluding "…data held by public undertakings, data held by public service broadcasters and their subsidiaries, data held by cultural establishments and educational institutions, data protected on the basis of national security and defense, and data falling outside the scope of the public sector bodies" public tasks.

Article 5 defines the requirements for data reuse, under the principles of non-discrimination, transparency, proportionality, and proper justification without efforts to limit competition. To guarantee data security, public sector organizations must ensure that personal data is anonymized, and commercially sensitive material is appropriately updated, aggregated, or otherwise managed with suitable disclosure restrictions.

The start of the application of the DGA will demand certain resources and institutional development in many of the Member States to reach the level of ability to adequately comply with the provisions of the GDPR. In this regard, the Commission foresees a need for Member States to invest in equipping their institutions to meet the requirements, especially coming from data protection law, in situations where data is being re-used. The measures may include developing a range of tools and technical solutions as well as adequate contractual provisions. If a public sector organization cannot allow access to specific data for re-use, it should help the potential user of data in obtaining the individual's agreement to re-use their personal data or the approval of the data holder whose rights or interests may be impacted by the re-use.

To make more publicly owned data available for re-use, the DGA restricts its usage of exclusive data re-use agreements (in which a public sector organization offers such an exclusive license to one enterprise) to certain circumstances of public interest. Also, while public sector organizations may charge fees for permitting re-use, they need to make sure that such fees do not exceed the necessary expenditures. Moreover, public sector organizations should reduce or even eliminate fees to encourage re-use for scientific research and other non-commercial objectives, as well as by SMEs and start-ups.

5 Competences and Role of European Data Innovation Board

In order to foster better implementation of the new data governance rules, the Article 29 of the DGA establishes the European Data Innovation Board (EDIB). The purpose of EDIB, established primarily as an expert group, will be to assist the European Commission in coordinating the practices and policies related to open data and supporting the cross-sector data use.

EDIB will consist of representatives of the competent authorities for data intermediation services and the competent authorities for registering altruism organizations. It will also include the EDPB, EDPS, ENISA and representation form other relevant institutions and organizations with specific expertise. According to Article 29, upon establishment the Board will divided into several subgroups, including one for stakeholder involvement, which should include representatives from industries such as health, environment, agriculture, transportation, energy, industrial manufacturing, media, cultural and creative sectors, and statistics, as well as research, academia, civil society, standardization organizations, relevant common European data spaces, and other relevant stakeholders and third parties. Even though the name of this working group resembles the European Data Protection Board, as Papakonstantinou and de Hert observe, its competences and role are not comparable. Where the EDPB has distinct powers to issue opinions, guidelines, recommendations and practices, it also monitors and ensures correct application of certain aspects of the GDPR (Article 70.1) whereas the EDIB is confined to an advisory role, advising, assisting and proposing the guidelines – much closer to the mandate of the former DPD Article 29 Working Party.

6 Discussion

While its always important to emphasize that the protection of personal data as a fundamental right in the EU is one of the more prominent achievements of the EU legislative development, development of the digital economy is also a necessity in the transformational process of building a postindustrial, information society. Availability of data for use should be followed by the general rise of trust in data intermediaries data-sharing mechanisms across the EU.

The regulation in question is increasingly divergent - the GDPR places a strong emphasis on safeguarding personal information and the rights of data subjects. On the other side, the DGA and Data Act are more concerned with promoting data exchange and developing a market for data. The competing goals might result in circumstances where data sharing prevails over data protection, a situation where data

protection authorities may feel a need to renew efforts in understanding these conflicting issues, perhaps by focusing more on promoting and participating in risk assessment, a role understood even in data protection systems far removed from EU and the GDPR (Mantelero 2016).

An important question at this time is whether the provisions of the DGA will contribute to this need to increase trust, or not. Certain provisions of the DGA, such as the definitions of data holders, data users, data sharing, seem to be in conflict or create confusion in application with regard to principals and other provisions of the GDPR (EDPB-EDPS Joint Opinion 03/2021). The joint opinion also mentions the definition of metadata as problematic, as it may imply processing of data that still qualifies as personal data.

More substantially, there appears to be a lack of clarity about a necessary legal basis for processing, where provisions of DGA, especially Article 5.6, 7.2.c, 11.11 and 19.3 refer to permission as something other than the regulated legal basis for processing of personal data under Article 6.1. of the GDPR. Same goes for instances of DGA provisions which seemingly may refer to other than legal basis prescribed by the Article 6 of the GDPR – however, the wording of applicable DGA provisions does not support the notion for DGA to be establishing a new, separate legal basis for processing nor does it in any case meet criteria for such situation set forth in Article 6.3 of the GDPR. According to that provision, such DGA provisions would have to specify "..inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures etc."(Article 6.3.1 of the GDPR).

The EDPB and EDPS have also expressed concern on the lack of separation/distinction between personal data processing and processing of non-personal data in the provisions of the DGA, probably inspired by the provisions of the Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, understanding how regulation of such processing is based and inspired on a different and often incompatible set of principles compared to processing of personal data. This reinforces the observation that such DGA provisions may create a regime of uncertainty and undermine the goals of the GDPR and the system of data protection in EU in general.

7 Conclusion

The EU has adopted the Data Governance Act (DGA) and is developing the Data Act proposal in an effort to foster the sharing of data across industries and further develop European common digital market for data. While the purpose of these activities is to strengthen the European digital economy, there is always risk that new legislation might endanger the data protection requirements set by the General Data Protection Regulation. The DGA and the Data Act proposal are part of the efforts to create a single market for data and promote data sharing across different sectors and although these regulations have been developed with GDPR standards in mind, they contain controversial provisions which might create conflicting situations or cause data sharing to take precedence over data protection, an established fundamental right in the EU.

The concept of intermediaries as introduced by the DGA as a neutral third parties facilitating data sharing between data holders and users may add another layer of complexity to the data sharing process and increase the risk of personal data misuse or data breaches, regardless of the GDPR obligations which intermediaries will have to operate under. Experience with data protection practice in the first five years of the GDPR application has repeatedly shown that complexity and number of stakeholders in a processing operation increase the chance of data breaches, while at the same time increasing administrative and technical load on organization compliance structures.

Another encouraged concept by the DGA, data altruism – sharing data for public interest persons – is also a potential source of risk as there are no adequate guarantees that would ensure that the data subjects are aware of the implications of sharing their data which in turn may prevent users from efficiently exercising their rights under the data protection law. As both DGA and Data Act in substantial part rely on data subject consent, experience in practical application of the GDPR shows how obtaining and maintaining consent may be a challenging endeavor.

Achieving an adequate balance between data sharing and data protection is essential in the EU legislation for reasons of economic growth, better protection of fundamental rights while achieving goals of public interest and other social benefits, furthering the state of legal harmonization and consistency among Member States and increasing competitiveness. Data sharing encourages innovation and subsequently economic growth through easier access to valuable information which in turns allows for more innovative research and development of new products ad services. On the other hand the EU has a goal of creating a consistent legal framework which will efficiently promote and protect recognized fundamental rights, among them privacy and data protection as distinctive rights of individuals in the EU. Any legislative intervention needs to contribute to better trust among all relevant stakeholders – citizens, businesses and governments. Ensuring adequate protection and enforcement of data subject rights can only help create an environment where individuals are more likely to share their data.

References

De Hert, P., Papakonstantinou, V: “The new General Data Protection Regulation: Still a sound system for the protection of individuals?”, Computer Law & Security Review, 32(2), 179-194, 2016.

Papakonstantinou, V., De Hert, P.:“Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI“, European Law Blog: News and Comments on EU Law, europeanlawblog.eu, April 2021.

Mantelero, A.:”Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection”, Computer Law & Security Review, 32(2), p. 238-255, 2016.

Gonzalez Fuster, G:”The Emergence of Personal Data Protection as a Fundamental Right of the EU”, Springer, 2014.

Katulić, T., Vojković, G.:“From Safe Harbour to European data protection reform“, 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1447-1451, Opatija, 2016.

Ruohonen, J., Mickelsson, S.:"Reflections on the Data Governance Act", arXiv preprint arXiv:2302.09944, arXiv 2023.

Grafenstein, M.:"Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR)", HIIG discussion Paper Series No.2022-02

Gellert, R., Graef, I:"The European Commission’s proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing", TILEC Discussion Paper, ISSN 1572-4042, March 2021, Tilburg University

Van Loenen, B., Zevenbergen, J., de Jong, J. “Balancing open data and privacy in the design of the land administration domain model”, ISPRS International Journal of Geo-Information, 6(5), 137, 2012.

Voss, W. G.: "Cross-Border Data Flows, the GDPR, and Data Governance Cross-Border Data Flows, the GDPR, and Data Governance", Washington International Law Journal, 29 Wash. Int’l L.J. 485 (2020).

Wessels, B.:”Identification of the uses of open data for the development of new businesses”, Telecommunications Policy, 36(11), 997-1007., 2012.

EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), June 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en

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), L 152/1, 3.6.2022.

The 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; GDPR

Proposal for a Regulation of the European Parliament and of the Council on Harmonised rules on Fair Access to and Use of Data (Data Act), Com(2022) 68 Final, 2022/0047(Cod)