The right to access information under the GDPR

Maria Bottis*

Ionian University, DALMS,
Ioannou Theotoki 72, Corfu, Greece
Email: botti@otenet.gr
*Corresponding author

Fereniki Panagopoulou-Koutnatzi

Panteion University,
Leof. A. Siggrou 136, Athens, Greece
Email: ferenikipan@yahoo.gr

Anastasia Michailaki

Ionian University, DALMS,
Ioannou Theotoki 72, Corfu, Greece
Email: amichailaki@gmail.com

Maria Nikita

University of Macedonia,
Egnatias 156, Thessalonliki, Greece
Email: nikita_ma@yahoo.gr

Abstract: The present paper offers a critique of the General Data Protection Regulation in the realm of access to information. Even though the GDPR supports the constitutionally obvious position that the right to data protection does not outweigh other equally important rights, the enhanced protection of the right to the protection of personal data leads to the potential neglect of other constitutional rights, such as that of access to information. Data protection and access to information authorities should be established both on an EU, as well as at national level as a single authority. Scientific research must be facilitated through access to a multitude of information. The present article explores the question of data ownership and aims to propose a new system that will enhance access to information. A key tool of our research will be the comparative overview of existing legislative systems and a review of the different approaches in the case-law of independent authorities.

Keywords: access; information; General Data Protection Regulation; GDPR; data ownership; freedom of information.

Reference to this paper should be made as follows: Bottis, M., Panagopoulou-Koutnatzi, F., Michailaki, A. and Nikita, M. (2019) 'The right to access information under the GDPR', *Int. J. Technology Policy and Law*, Vol. 3, No. 2, pp.131–142.

Biographical notes: Maria Bottis is an Associate Professor of Information Law at the Ionian University, Greece. In 2000–2001 she was appointed as a Faculty Fellow at the Harvard University. She is the Director of the International Society for Ethics and Information Technology and she has instituted the International Conference on Information Law series.

Fereniki Panagopoulou-Koutnatzi is an Assistant Professor of Constitutional Law at the Panteion University, Greece. She served as a Legal Auditor at the Greek National Data Protection Authority for eight years and has published extensively on data protection and privacy issues.

Anastasia Michailaki is an Attorney-at-Law and independent researcher. Her PhD research focuses on the application of the internet of things and personal data.

Maria Nikita is a computer scientist whose research concentrates on privacy and data protection in RFID technology.

This paper is a revised and expanded version of a paper entitled 'Modern intellectual property governance and openness in Europe: a long and winding road?' presented at the 8th International Conference on Information Law and Ethics 2018, Antwerp, 13th–14th December 2018.

1 The problematics

The new General Data Protection Regulation 2016/679 (GDPR) of the European Union and the extensive publicity it has received over the past months, obviously co-driven by the fear of severe penalties in case of its infringement, have enhanced awareness and sensitivity around data processing. At the same time, the other objective of the GDPR, which concerns the protection of the free movement of personal data within the Union, has not received the same level of attention, at least not in common perception.

According to Recital No. 4 of the GDPR,

> "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This regulation respects all fundamental rights and observes the freedoms and principles recognized in the charter as enshrined in the treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

In the same spirit, Art. 85 of the GDPR states that, "Member States shall by law reconcile the right to the protection of personal data pursuant to this regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression."

In this respect, the GDPR does not constitute a novelty. In fact, it is an updated version of Directive 95/46/EU "on the processing of personal data and on the free movement of such data", which contains the same fundamental principles and sets both

the protection and the movement of personal data on an even playing field (Alexandropoulou, 2016). The Directive did not seek to establish an absolute and indisputable right to personal data protection in order to further promote the right to privacy: its objective was to liberate the movement of data within the Union in order to support the free movement of goods, capital, services and labour, to the extent permissible by the fundamental right to privacy.[1]

Thus, the right to information and the right to the protection of personal data should, primarily, be seen as complementary, equal rights and weighed against each other only if they cannot co-exist. Even though both the previous and the new regulatory framework clearly state that personal data protection should be balanced against other fundamental rights, there are strong indications that this is oftentimes not the case.

There is concern that our enthusiasm for personal data protection has led to the neglect of other constitutionally protected rights. The right to data protection does not, and should not, per definition, prevail over other constitutional rights, such as the right to information and the freedom of expression. In other words, it is not an absolute and tyrannical right that dominates all others.

It is not just our enthusiasm that justifies what, at times, appears to be as an almost 'by default' protection of personal data over other constitutional rights. This enthusiasm could also be explained by the need for cost and time efficiency. If, for example, a number of data subjects demand that their personal data be erased by an online newspaper, it is, in all likelihood, far quicker and thus cheaper for the newspaper to comply with those requests, rather than to justify their refusal by weighing those demands against other constitutional rights on a case by case basis.

In the same spirit, the perceived imperative need to protect personal data that has emerged has also led to a widespread refusal to provide information. Personal data is commonly 'protected' abusively, as an excuse and an obstacle to the exercise of the right to information.

Experience has shown that the most problem-free choice on the part of data controllers is simply to refuse the disclosure of data that have been requested. The simple reason for this is because an eventual unjustified provision of data will be punished far more stringently than a potential case of unjustified lack of disclosure. The time has, indeed, come to disclose and resolve this unjust legal situation, threatening constitutional rights of citizens throughout Europe.

2 The freedom of access to information under the GDPR – comparative study

The application of the GDPR is mandatory for EU Member States and the discretion granted to them lies only in the application of the requirements under the national data protection regimes (European Parliament and the Council, 2016). The exceptions on data processing provided by the GDPR refer to the exercise of the freedom of expression and right to information, or to archival and research purposes, leaving Member States to address these in their national legislation. The freedom of access to information is a right that has to be expressly mentioned in the aforementioned exceptions with respect to the Chapter of Fundamental Rights of the EU (Human Rights Watch, https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation).

The legislative framework of the Member States that have incorporated the relevant provisions on the access to information under the GDPR in their national legislation is set out below.

2.1 Bulgaria

The action plan of the Bulgarian Data Protection Authority contains a strategic objective relating to certain services provided to citizens and data controllers, which concerns an accessibility policy aimed at facilitating access through e-government, administrative services and open data approach (Republic of Bulgaria, Commission for Personal Data Protection, http://www.cpdp.bg).

2.2 Estonia

The Data Protection Inspectorate defends the public's constitutional right to have access to the activities of public authorities. The Inspectorate is empowered by the Public Information Act, which provides the guarantee that every person may access information intended for public use, based on the principles of democracy and open society (Estonian Data Protection Inspectorate, http://www.aki.ee/en/inspectorate).

2.3 Malta

The Maltesian Data Protection Act has issued a Code of Practice for Public Authorities, based on the Freedom of Information Act (Cap. 496), Article 41, that came into force on the 1st of September 2012. According to this Code, each Public Authority should nominate a Freedom of Information Officer and at least one Alternative Freedom of Information Officer, who will be responsible for the requests relating to documents and information, in line with the Freedom of Information Act (Office of the Information and Data Protection Commissioner, https://idpc.org.mt/en/Pages/foi/publications.aspx).

2.4 Slovenia

According to the Slovenian Data Protection Authority's access to information, the Slovenian people have access to public information, as a matter of law. They are under no obligation to justify their legitimate interest for their search, or to explain the purpose of use of the related information. There is only one exception, namely that of the re-use of the information obtained, as citizens have the obligation to mention the purposes of the re-use (Republic of Slovenia, Information Commissioner, http://www.ip-rs.si/en/freedom-of-information/access-to- information/my-rights).

2.5 Croatia

With the Law on Amendments to the Law on the Right of Access to Information adopted by the Croatian Parliament on the 22nd of December 2010, the Croatian Personal Data Protection Agency obtained jurisdiction over the Law on the Right of Access to Public Information. Some of the most important responsibilities of the agency concerning access to information are the following:

- to supervise the enforcement of the law on access to information
- to resolve complaints on the right to access to information
- to train Information officers in public bodies
- to collect and analyse the annual reports of public bodies on requests for access to information
- to create an annual report on the enforcement of the law on access to information (Croatian Personal Data Protection Agency, http://azop.hr/projects/agency/cappd-taiex-worksho).

2.6 Latvia

In Latvia, the Freedom of Information Law has been adopted so as to facilitate public access to information. The law sets out a very specific procedure under which natural and legal persons have the right to obtain information from state, administrative and local institutions, as well as on how the information obtained may be used. No public interest needs to be justified by the citizens (Data State Inspectorate of Latvia, http://www.dvi.gov.lv/en/legal-acts/freedom-of-information-law/).

2.7 UK

The Information Commissioner's Office (ICO) helps the organisations comply with the Freedom of Information Act, the Environmental Information Regulations, the INSPIRE Regulations, the re-use of Public Sector Information Regulations and the associated codes of practice. When the aforementioned legislation is not applied by the authorities or the public sector bodies, the ICO may take the following action:

- check the compliance of the organisations with the aforementioned legislation, especially the Act
- issue information notices to the authorities to improve their compliance
- serve enforcement notices in cases of infringement of the Act
- issue recommendations towards compliance
- issue decision notices resulting from the investigation of a specific request
- prosecute the criminal offenders under the Act
- report to Parliament concerning freedom of information issues (ICO, http://ico.org.uk/about-the-ico).

2.8 The Freedom of Information Act 2000

Public access to information provided by the Act is affected in two ways:

- public authorities have the obligation to disclose information about their work
- citizens have the right to request information from public bodies.

The information covered by the Act and the Act itself are applied in England, Wales and Northern Ireland.

The public authorities that are bound by the Act are government departments, local authorities, the NHS, state schools and police forces.

The information provided by citizens under the Act is not their personal data – in this case the person makes a request under the GDPR. The Act examines of the information needed refers to personal data if third parties and whether the disclosure of the personal data of the third parties would constitute a breach of the principles of data protection. In any case, it is necessary to strike a careful balance between transparency under the Freedom of Information Act, and the data subject's right to privacy under the Data Protection Act. Following that, it can then be decided whether information can be granted without violating data protection principles (ICO, https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/).

In addition to the above countries that have established provisions on access to information under the GDPR rules, a few more EU Member States that provide access to information for journalistic, scientific, artistic or literary purposes only, are as follows:

2.9 Austria

Section 9 of the Austrian Data Protection Act has special provisions on the processing of personal data under the freedom of expression and right to information. According to these provisions, several regulations of the GDPR (especially those on the rights of data subjects) are not applicable to the processing of personal data for journalistic, scientific, artistic or literary purposes (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.10 Belgium

A large number of GDPR provisions are declared inapplicable or only conditionally applicable when it comes to processing for journalistic, scientific, artistic or literary purposes. In this respect, 'journalistic purposes' are considered to cover the preparation, collection, drafting, production, distribution or archiving for the purpose of informing the public, using any media and where the controller should ensure compliance with journalistic ethics (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.11 Czech Republic

Section 16 of the Data Protection Act allows processing of personal data for journalistic purposes or for purposes of academic, artistic or literary expression. Sections 17 et seq. stipulate exceptions to right to information obligations (Section 17), protection of source and content of information (Section 18), exceptions to the right to restriction of processing (Section 19), information about rectification and erasure (Section 20), and limitation of the right to object (Section 21) (Bird & Bird,

https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.12 Finland

According to Section 27 of the Data Protection Act only limited provisions of the GDPR apply to the processing of personal data for the purposes of journalistic, academic, artistic or literary expression. This approach upholds the situation as it was under the abrogated Personal Data Act (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.13 France

Article 40 of Law No. 78-17 of the 6th of January 1978 relating to information technology, files and individual freedom, was not amended. The use of the right to erasure («right to be forgotten») can be denied when the processing of data is necessary for the exercise of the freedom of expression and right to be informed (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.14 Germany

Paragraph 35 of the new German Federal Data Protection Act ('FDPA') exempts the controller from his/her obligation "to erase personal data where the erasure is, in case of non-automatic data processing, impossible, or only possible with disproportionately high effort and the data subject has a minor interest for erasure." Paragraph 27(2) of the FDPA restricts the data subjects' rights subject to certain further requirements (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.15 Ireland

Under Section 43(1) of the Data Protection Act, the processing of personal data, pursuant to the right to freedom of expression and information (including processing for journalistic purposes or for the purposes of academic, artistic or literary expression), should be an exemption from the provisions of the GDPR that are incompatible with such purposes (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.16 Italy

No deviations from the GDPR are in place. On the basis of the provisions of the Scheme, the Code of Practice concerning the processing of personal data in the exercise of journalistic activities (Annex A of the Italian Data Protection Act) will remain in force (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.17 Netherlands

The UAVG provides that there is no application of the Act in respect of personal data processing for journalistic purposes or for the purposes of academic, artistic or literary expression. Article 41 of the GDPR Execution Act provides that the GDPR Execution order does not apply where personal data are processed exclusively for journalistic purposes or for the purposes of academic, artistic or literary expression. In addition, it includes a list of chapters and articles in the GDPR that are also not applicable for these purposes, namely:

a Article 7(3), 11(2)

b Chapter III

c Chapter IV (with the exception of Articles 24, 25, 28, 29 and 32)

d Chapter V

e Chapter VI

f Chapter VII.

Article 41 of the UAVG limits the scope of certain obligations in connection with (compelling) general interests, in line with Article 23 of the GDPR. Therefore, it provides for exceptions to the rights of the data subject and the duties of the controller. The GDPR (Arts. 12–21 and 34 GDPR) does not apply, in part (insofar as this is deemed to be appropriate and proportionate) to data processing in view of – inter alia – important public interest objectives, public security, the protection of the data subject or of the rights and freedoms of others; and/or for the collection of civil claims (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.18 Poland

The Polish Data Protection Act provides that some provisions of the GDPR will not apply in case of personal data processing for journalistic purposes or for the purposes of academic, artistic or literary expression (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.19 Slovakia

The New Data Protection Act stipulates in Article 78 that personal information may be processed without a data subject's consent for journalistic, academic, artistic and literary purposes. Nevertheless, such processing must not breach a data subject's right to personality protection and privacy (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

2.20 Sweden

The GDPR and the Data Protection Act should not be applied to the extent that this would breach the laws on the freedom of expression (Paragraph 1:7 of the Data Protection Act). The Data Protection Act provides that Articles 5–30 and 35–50 of the GDPR should not be applicable to the processing of personal data for journalistic purposes or for purposes of academic, artistic or literary expression (Bird & Bird, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression).

3 Data ownership

The question of 'who owns my data?' is an important issue that researchers have been attracted to in recent years. In our days, organisations have more data than ever before. Individuals increasingly share more data on the internet in exchange for services, so any of these personal and non-personal aspects of their daily activities may be picked up and stored as data by companies and governments alike. Consequently, the amount of data collected and processed is substantially outsized (Al-Khouri, 2012).

In order to understand the legal concept of data ownership, it is, first of all, necessary to understand the meaning of ownership and the definition of data. In general terms, ownership (Definition of Ownership, https://en.wikipedia.org/wiki/Ownership) recognises a number of rights and grants control to a person over a property. This property may be an object, real estate or intellectual property and the rights over this property can be transferred from one person to another. Also, data can be defined as what is being used to provide information and, in turn, the legal concept of data ownership (Definition of Data Ownership, https://en.wikipedia.org/wiki/Data_ownership, https://www.techopedia.com/definition/29059/data-ownership) recognises legal rights and complete control to a person over a group of data (European Commission, 2016).

On the one hand, data ownership relates to issues like data management and control, such as privacy, trust and security (Janeček, 2018) but, on the other hand, data ownership is considered as a legal and contractual barrier to the development of the data economy and the use of the internet of things, robots and autonomous systems (European Commission, 2018b).

According to Scassa (2018), "ownership claims and legal skirmishes over rights to own or control data" occur in various cases. Moreover, data ownership can play a part in commercialising data, create monopolies, have public dimensions and be challenging to locate, whilst it may also play a role in privacy protection too.

At the same time, data are divided into personal data and non-personal data. With regard to personal data, the GDPR (Article 4) provides the definition (Scassa, 2018), so someone could imply that the remaining are non-personal data. Nevertheless, the definition is quite broad and, in reality, the distinction of data as personal and non-personal data is not an easy one, as non- personal data can actually help to generate personal data (Drexl, 2019).

The free flow of data enhances innovation and is considered a key for the growth of the data economic. The GDPR covers only the case of ownership of personal data and does not deal with the ownership of non-personal data at all. As a result, the EU had to adopt new rules on the free flow of non-personal data and, consequently, in December 2016 it addressed a letter to the President of the European Council, calling for a legislative proposal to end data localisation practices (European Parliamentary Research Service, 2018).

A year later, the Commission proposed a regulation so as to address the barriers to the free movement of non-personal data across borders. Moreover, this proposal (European Commission, 2017) aimed at improving the movement of non-personal data across borders in the single market, ensure that requests from competent authorities on getting access to data for regulatory control purposes were being accepted and simplify the procedure of changing service providers and porting data for professional users of data. Finally, in 2018 the Council adopted the regulation (European Parliament and the Council, 2017) on a framework for the free flow of non-personal data in the European Union, which is expected to improve the competitiveness of Europe.

According to the vice-president for the Digital Single Market, Andrus Ansip, and Commissioner for Digital Economy and Society, and Mariya Gabriel,

> "A digital economy and society cannot exist without data and this regulation concludes another key pillar of the Digital Single Market. Only if data flow freely can Europe get the best from the opportunities offered by digital progress and technologies such as artificial intelligence and supercomputers. This Regulation does for non-personal data what the General Data Protection Regulation has already done for personal data: free and safe movement across the European Union." (European Commission, 2018a)

4 Conclusions

The GDPR accepts that personal data protection is not an absolute right. Unfortunately, however, the GDPR passed on the prime opportunity to set out the appropriate conditions and structures for the establishment of protection authorities that would guarantee the equal and simultaneous exercise of the two constitutional rights in question. From the review of national legislation, we see that national legislators did not seize the opportunity to change Data Protection Authorities into Data Protection and Access to Information Authorities. Access to information and personal data protection must operate, primarily, in a complementary manner, giving no precedence to one or the other. Nevertheless, a careful balance between them is often the only way to ensure the proper administration of justice in the event of conflicting, yet deserving interests related to data protection and the right of access to information.

Acknowledgements

Work co-funded by Greece and the European Social Fund (ESF) through the Operational Program "Human Resources Development, Education and Lifelong Learning" for the implementation of the ESF & the Youth Employment Initiative in Greece.

References

Alexandropoulou-Egyptiadou, T. (2016) *Personal Data*, Nomiki Vivliothiki.

Al-Khouri, A.M. (2012) 'Data ownership: who owns 'my data'', *International Journal of Management & Information Technology*, Vol. 2, No. 1, pp.1–8.

Bird & Bird [online] https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression (accessed 20 March 2019).

Croatian Personal Data Protection Agency [online] http://azop.hr/projects/agency/cappd-taiex-workshop (accessed 20 March 2019).

Data State Inspectorate of Latvia [online] http://www.dvi.gov.lv/en/legal-acts/freedom-of-information-law/ (accessed 20 March 2019).

Definition of Data Ownership [online] https://en.wikipedia.org/wiki/Data_ownership (accessed 12 January 2019), https://www.techopedia.com/definition/29059/data-ownership (accessed 20 March 2019).

Definition of Ownership [online] https://en.wikipedia.org/wiki/Ownership (accessed 20 March 2019).

Drexl, J. (2019) 'Legal challenges of the changing role of personal and non-personal data in the data economy', in Franceschi, A. and Schulze, R. (Eds.): *Digital Revolution – New Challenges for Law*, Intersentia, Max Planck Institute for Innovation & Competition Research Paper Nos. 18–23 [online] https://ssrn.com/abstract=3274519.

Estonian Data Protection Inspectorate [online] http://www.aki.ee/en/inspectorate (accessed 20 March 2019).

European Commission (2016) *Legal Study on Ownership and Access to Data (SMART Number 2016/0085)* [online] https://ec.europa.eu/digital-single-market/en/news/legal-study-ownership-and-access-data-smart-20160085 (accessed 20 March 2019).

European Commission (2017) *Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union* [online] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46830 (accessed 20 March 2019).

European Commission (2018a) *Joint Statement by Vice-President Ansip and Commissioner Gabriel on the European Parliament's Vote on the New EU Rules Facilitating the Free Flow of Non-Personal Data* [online] http://europa.eu/rapid/press-release_STATEMENT-18-6001_en.htm (accessed 20 March 2019).

European Commission (2018b) *Study on Emerging Issues of Data Ownership, Interoperability, (Re-)usability and Access to Data, and Liability* [online] https://www.wik.org/fileadmin/Studien/2018/EU_Data_ownership_en.pdf (accessed 20 March 2019).

European Parliament and the Council (2016) *General Data Protection Regulation* [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed 20 March 2019).

European Parliament and the Council (2017) *Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union* [online] http://data.consilium.europa.eu/doc/document/PE-53-2018-INIT/en/pdf?lspt_context=gdpr (accessed 20 March 2019).

European Parliamentary Research Service (2018) *EU Legislation in Progress. Free Flow of Non-Personal Data in the European Union. Briefing* [online] http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614628/EPRS_BRI(2017)614628_EN.pdf (accessed 20 March 2019).

Human Rights Watch [online] https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation (accessed 20 March 2019).

Information Commissioner's Office (ICO) [online] http://ico.org.uk/about-the-ico (accessed 14 January 2019).

Information Commissioner's Office [online] https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what- is-the-foi-act/ (accessed 20 March 2019).

Janeček, V. (2018) 'Ownership of personal data in the internet of things', *Computer Law & Security Review*, Vol. 34, No. 5, pp.1039–1052.

Office of the Information and Data Protection Commissioner [online] https://idpc.org.mt/en/Pages/foi/publications.aspx (accessed 20 March 2019).

Republic of Bulgaria, Commission for Personal Data Protection [online] http://www.cpdp.bg (accessed 20 March 2019).

Republic of Slovenia, Information Commissioner [online] http://www.ip-rs.si/en/freedom-of-information/access-to- information/my-rights (accessed 20 March 2019).

Scassa, T. (2018) *Data Ownership*, CIGI Papers No. 187 [online] https://ssrn.com/abstract=3251542 (accessed 20 March 2019).

Notes

1 Within this framework, the considerations of Recitals 3, 8 and 10 of the Preamble of Directive 95/46/EU, stipulating the following, is of the essence:

> "(…) (3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded; (…) (8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas community action to approximate those laws is therefore needed; (...) (10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community Law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the community."