GDPR and the Reuse of Personal Data in Scientific Research

doc. dr. sc. Tihomir Katulić

Faculty of Law of the University of Zagreb,
Trg maršala Tita 14, Zagreb, Croatia
E-mail: tihomir.katulic@pravo.hr

Anita Katulić

National and University Library in Zagreb
Hrvatske bratske zajednice 4
E-mail: akatulic@nsk.hr

ABSTRACT - Impact of EU data protection reform on reuse (secondary use) of personal data in scientific research has been largely ignored by the scientific community when compared to other effects and consequences of new legislative framework on various business and governmental activities and general use of personal data in social processes. The new legislative framework contains distinct new mechanisms and provisions concerning reuse of personal data for research purposes and will foster new practices and facilitate a more efficient and economic approach to various fields of research. Research institutions, libraries and archives recognized as data controllers need to comply with the new regulation. This paper will discuss selected topics from the field of new data protection regulation, especially organizational practices in order to ensure information security and accountability of these organisations.

Keywords: GDPR, data protection, libraries, digital archives, privacy

I. Introduction

When the new General Data Protection Regulation officially goes into effect in May later this year, it will mark a turning point in almost a quarter of a century of data protection development in the European Union. [1]

A lot has changed since the first adoption of data protection rules on the European level in the early 1990's through the provisions of the Data Protection Directive. [2]

Rapid technological development, particularly of electronic communications, the Internet, search engines, social networks, new information society services and postindustrial data economy, especially in the online content industries, have brought around new and unforeseen challenges for the protection of personal data of EU citizens and all other physicial persons residing or travelling through EU. The scale, the speed and the ubiquity of processing have increased dramatically.

What has also changed is the legal status of personal data protection in the EU legal system. The Treaty on the Functioning of the EU establishes personal data protection as a right available to all individuals in the EU. [3]

Article 8 of the Charter of Fundamental Rights of the EU enshrines personal data protection as a distinct fundamental right under Title II of the Charter, equivalent to right to liberty and security, respect for private and family life (privacy), freedom of thought, expression, assembly etc.[4]

Regulating how personal data is obtained, processed and retained, the new Regulation will affect organizations from EU and abroad that make use of personal data obtained from physical persons in the EU.

Twenty three years after enacting the Data Protection Directive, a milestone in legal development of personal data protection in 1995, and almost six and and a half years after the first regulation proposal, and following two years of *vacatio legis* period left for Member Countries to prepare for its application, the General Data Protection Regulation is now ready to come into effect bringing both evolutionary and revolutionary mechanisms to protect individual's rights concerning their personal data.

II. From Directive To Regulation

Replacing the earlier Data Protection Directive and the national laws it was transposed into, as the new source of the EU material rules concerning data protection principles, users rights and protection mechanisms the Regulation has several main goals.

One of them is to ensure adequate protection of the fundamental data protection principles and rights of individuals subjected to personal data processing such as the right to be informed about data processing, right to access own personal data, right to erase or transfer personal data to another data controller etc.

The Regulation contains mechanisms to ensure adherence to basic principles of data protection such as lawfulness, fairnes and transparency of processing, purpose limitation, data minimisation, accuracy, storage limitation, preservation of integrity and confidentiality and especially, to make sure the controller remains responsible and is able to demonstrate compliance through the principle of accountability.

Another is to update the existing framework that has not kept proper pace with the evolving technology landscape

that has progressed immensely over the last quarter of the century. The advent of technologies allowing cheap and quick DNA sequencing, detailed biometry readings and other technologies that reveal sensitive health may potentially lead to abuses and discrimination of affected individuals.

The choice of the delivery method, a Regulation instead of a Directive, reveals the need to improve uniformness and adherence to data protection standards across the 28 Member States.

By direct application rather than having each Member State decide how its requirements are to be transposed into nation law, the Regulation will help enforce common EU standards of data protection regardless of the legal system, state or supervisory body that interprets it.

The Regulation however leaves some room Member States to regulate their specific supervisory system, provide additional rules alongside or over the standards of the GDPR and clarify potentially unclear concepts such as legitimate interest as the legal basis of processing, required data protection officer skillset and expertise, privacy impact assessment methodology, liability of persons responsible for data controllers actions, provisions regarding collective redress after a data breach and so on.

As of the moment of writing, only five of the Member States have adopted national laws accompanying the GDPR while additional fifteen have produced draft proposals. [5]

The draft of the new Croatian Law on Implementation of the GDPR is currently available to the public. It does not contain provisions regarding the exceptions, safeguards and derogations relating to processing for scientific research purposes as regulated by the Article 89. of the GDPR.

III. Key Concepts and Definitions

There has been much discussion regarding the key definitions of terms regarding data processing in relation to existing laws and the Data Protection Directive. Some authors point out to more elaborate definitions concluding that their scope has expanded. Some claim the scope has not changed.

One of the most important ones is the definition of personal data. The Data Protection Directive used to define personal data as any information relating to an identified or identifiable natural person, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [6]. We can find similar provisions in a host of national laws such as the Article 2 of the Croatian Personal Data Protection Act [7].

The GDPR expands the definition referencing identifiers 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, but does not broaden it – the original definition has always implied that any information relating to an identified or identifiable natural person represents personal data, regardless of whether categories of such information have been explicitly named by the relevant laws or not.

Similarly, with regard to the definition of special categories of personal data, especially health data, there is still some confusion whether biometric and genetic data, now explicitly defined by the GDPR, represent an extension of existing special categories of data. They do not – they represent of course data pertaining to health of data subjects, and such data is already recognized as special category of personal data by existing regulation. What is new is special reference to biometric data with the purpose of uniquely identifying a natural person.

IV. Special Cathegories of Personal Data

The GDPR recitals commenting on the Article 9 of the GDPR state that Member States should be allowed to maintain or introduce further conditions, including limitations with regard to processing of genetic data, biometric data or health data in general while not hampering the free flow of personal data within the Union should those provisions apply to cross-border processing of such data. [8]

The draft of the Croatian GDPR implementing law contains four articles concerning genetic and biometric data, providing additional safeguards regarding use of genetic data in life insurance contracts, use of biometric data by public and private sector authorities for the purposes of protection of persons, property, classified or business secrets [9]

In addition to principles of data protection recognized by the previous generation of laws starting with the Data Protection Directive, the Regulation now explicitly regulates the need to ensure the integrity and confidentiality of personal data during the collection, processing, use and retention.

These principles are easily recognized by information security experts as two of three founding principles of information security, the CIA triad of confidentiality, integrity and availability. [10]

From the perspective of research organisations, libraries and archives, the main changes for these organisations include requirement to implement adequate procedures for responding to user request in connection with their rights as data subjects, implement privacy by design and privacy by default measures, technical and organisational measures to reduce risk, conduct privacy impact assessments, develop adequate incident reporting procedures and regulate the position and responsibilities of the data protection officers.

While most organisations are aware of the Regulation's very strict fines, very few are aware of the reinforced liability for damages in case of data breaches in the context of possible collective redress and the personal liability of management and board members as regulated by national laws.

IV. Reuse of Personal Data in the Context of Research

Information systems of various research organisations these days contain a wealth of personal information that could be reused and lead to important discoveries in all fields of science. Use of this data potentially could allow researchers to uncover new knowledge concerning today's medical, social and economical challenges.

In general, Article 5 of the GDPR regulating the principles relating to processing of personal data allows the retention of personal data longer than necessary for the

purposes of for which the personal data was originally collected and processed if needed for archiving purposes, scientific and historical research purposes or statistical purposes and if appropriate technical and organisational measures are applied. This abrogation of the principle of storage limitation is further regulated by the Article 89 and several recitals. [11]

The Regulation considers the reuse of personal data collected in various situations where the purpose of initial collection does not cover the possible use in research.

Recital 50 of the Regulation considers the use of personal data for purposes different than those at the time of initial collection, stating that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations meaning that these uses do not represent a change in purpose of processing that would require a separate legal basis.

Furthermore, Recital 156 of the GDPR, reflecting on the provisions of Article 89 comments the obligation to ensure appropriate safeguards – technical and organisational measures – to ensure the rights and freedoms of data subjects in the case of reuse of data for purposes of archiving in public interest, scientific and historical research purposes or statistical purposes.

Article 89 regulates that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. What these appropriate measures are, the Regulation does not specify above a passing comment on the possibility of use of pseudonymisation techniques.

Instead, general obligation is put forth that data controllers need to implement technical and organisational measures to ensure respect for the principle of data minimisation and anonymize data if secondary processing no longer requires the identification of data subjects.

Article 89 is also interesting as it leaves to the Union and Member States manouvering room to implement serious derogations from the data subject rights regulated in Articles 15, 16, 18 and 21 of the GDPR – right of access, rectification, restriction of processing and the right to object to (automated) data processing and profiling. How will these derogations look and function in practice, remains to be seen if and when they are adopted in the next generation of Member States data protection laws.

Another way research institutions, libraries and archives can further process personal data for research purposes is through obtaining a valid consent as the legal basis for processing.

Under the GDPR, rules for obtaining consent are more detailed and demand that consent be given by a clear, affirmative act by an individual informed specifically on the categories of data and their use.

The request for consent needs to be presented in a separate form and manner distinguishable from other contract matter and presented in a clear and plain language that informs the data subject of his rights.

Finally, the controllers need to be able to demonstrate how, when and what has data subject consented to with regard to processing of their personal data. [12]

V. DPO AND DPIA: KEY MECHANISMS TO SAFEGUARD DATA SUBJECT RIGHTS

One of the key new features of the GDPR is a risk-based approach to data protection activities directing data controllers to put into practice technical and organizational measures to protect personal data according to the percieved level of risk. [13]

The Regulation differentiates between three levels of risk and corresponding obligations for the controllers as regulated by the GDPR: high, normal or intermediate and low risk.

A high-risk processing activity requires that organizations engaging in such activity conduct data protection impact assessments. Should a personal data breach occur that could result in a high risk to the rights and freedoms of natural persons, the controller has an obligation to communicate the data breach to the data subject without undue delay.

Most of personal data processing activities will not fall under the high-risk category. For these activities, the controller should adopt measures appropriate to the perceived level of risk.

Finally, some of the activities will present minimal risk towards the rights of data subjects and in these situations controllers are relieved from obligations to notify supervisory authorities or data subjects in case of a data breach.

Research institutions, libraries and archives should assess their legal basis for processing personal data and record processing activities inline with the provisions of the Article 30 of the GDPR. Establishing a record of processing activities, categories of personal data collected, their use and possible exports, categories of individuals, identifying information systems containing personal data and assessing risks to individuals and their rights are the first steps in a compliance program.

The DPIA is a process aimed at assessing the likelihood and severity of risk of a data processing activity from the perspective of individuals rights and freedoms and suggesting mitigation measures to lower risk. It is designed to describe the processingm assess its necessity and proportionality and help manage risks. DPIA represents an important tool for demonstrating accountability and compliance with the Regulation. [14]

While carrying out a DPIA is not mandatory for every processing operation, Article 35 of the GDPR determins the situations where data controllers are mandated to implement a data protection impact assessment (DPIA) of one or more of their data processing activities.

The Regulation mandates conducting DPIAs where new technologies are used, for example in biotechnology, genome sequencing, complex personal data profiling and data set combining, where systematic and extensive processing of special categories of personal data is being performed and where there is a systematic monitoring of a publicly accessible area on a large scale.

From the perspective of research institutions, libraries and archives, all these situations may already account for significant amount of their personal data processing. While the national supervisory authorities are expected to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection

impact assessment, they may also establish and publish a list of the kind of processing operations for which no data protection impact assessment is required. A typical situation concerning research data where DPIA is likely to be required is archiving pseudonymised personal sensitive data such as data concerning vulnerable data subjects of research projects or clinical trials.[15]

The DPIA process is not a once in a process life-cycle procedure but instead a continuing activity that controllers need to perform when conditions and circumstances of processing change, especially concerning the risk to individual's rights and freedoms.

At the same time, under the GDPR, the regulation of the position, roles and duties of data protection officer has been significantly enhanced. Article 37 of the GDPR regulates the situations where appointment of data protection officer is mandatory, emphasizing the processing done by public authorities or bodies and controllers whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale or processing on a rage scale of special categories of data and personal data relating to criminal convictions and offences.

While the concept of DPO in itself is not unfamiliar to data protection regulation, Data Protection Directive did not require organisations to appoint a DPO. The practice of appointing the DPO has developed in national legal systems of Member States over the last fifteen years.

Regarding the data protection officer's required professional qualities and expert knowledge, Article 37.5 of the Regulation states that the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

The DPO has to be able to fulfil the tasks set by the Article 39 of the Regulation, especially to inform and advise the controller or the processor and the employees who carry out processing of their data processing obligations.

The DPO also needs to monitor compliance with the GDPR and other Union and national laws and with the policies of the controller or processor in relation of the protection of personal data. He or she will participate in awareness-raising and training of staff involved in processing operations and the related audits, provide advice where requested as regards the data protection impact assessment and monitor its performance, cooperate with the supervisory authority and act as the contact point for the supervisory authority on issues relating to processing while paying due care to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. [16]

VI. Practical Implications On Research Institutions

Research institutions, libraries and archives by definition collect and use substantial amount of data that may contain personal data.

While the Regulation confirms and explicitely protects data subject rights, it also states that right to protection of personal data is not an absolute right and that it has to be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality, i.e. in the case of balancing against rights regulated by the Articles 9 and 10 of the Charter of Fundamental Rights of the EU.

With already mentioned provisions of Art. 89 and Recital 153 of the GDPR, the Member States are allowed to develop specific solutions to the balancing between these rights. [17]

Unlike the earlier data protection laws, the GDPR now applies not only to research institutions, libraries and archives in the EU, but also to organizations established elsewhere provided that they collect and use personal data or monitor data subjects residing in the EU.

Even though GDPR expands the possibility of research institutions to reuse personal data, the research organizations, just like any other data controllers or processors need to meet the new regulatory obligations.

In practice, this means several key efforts inluding education, personal data maintenance and discovery, compliance (gap) analysis and implementation of adequate technical and organisational measures.

Education should include not only researchers and other key personnel handling personal data, but also management and data protection officers if they have been appointed. Data protection is still not widely accepted as a mandatory part of legal education in most European universities and is even less present in other professions and higher education programs.

In order to satisfy regulatory requirements all organisations subject to the GDPR need to conduct activities to adopt or modify their data usage, security and privacy policies.

In order to do so, they need to have an informed overview of personal data processing activities and ensure adequate protection measure and establish clear and practical procedures concerning users' rights requests, data breach incident response and reporting procedures, data protection impact analysis etc.

Research organisations, libraries and archives may in the course of their activities use outside resources or outsource some of the data processing to third parties. If personal data is also processed in this manner then special care needs to be observed when dealing with data processors and ensuring that obligations regulated by the Article 28 of the GDPR are observed by the data controller and the processor. This means a thorough review of procedures and contracts governing these activites.

This review should include an information system and information security audit both of the data controller's systems and those of the processors.

After concluding the analysis of the existing state of data protection, the data controllers should implement measures to adapt their processing to GDPR requirements starting from deletion of redundant and superfluous data, risk analysis of current and planned processing operations, appointment of the data protection officer and his proper positioning in the organisational structure with regard to provisions of Article 38 as well as the issues concerning possible conflict of interest etc.

VII. Open Questions

From the perspective of research institutions and libraries, there are still a few uncertainties left before the Regulation enters into effect.

One of them concerns the data library systems use to globally exchange data on newly published books and other publications, which usually contain personal data on authors and other individuals and require export of data into third countries and international organizations that will not meet the future adequacy decision requirements as regulated by the Chapter V of the GDPR.

Second issue concerns the efforts to reconcile the rules that govern freedom of expression, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data.

The Regulation states that processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to appropriate derogations or exemptions if there is a need to reconcile the right to the protection of personal data with the right to freedom of expression and information as regulated by the EU Charter of Fundamental Rights.

The Regulation Recitals specifically refer to the issue of processing of personal data in the audiovisual files and in the the news and press libraries and archives, requiring Member States to adopt adequate provisions to allow exemptions and derogations required to balance these fundamental rights.

An issue that is already present in the provision of Article 39 concerns the possibility of bringing a collective redress action against the data controller, as recommended by the European Commission in 2013.

The provision allows data subjects to collectively assign a non-profit institution to file a complaint and pursue rights from Articles 77, 78 and 79 of the GDPR including a right to an effective judicial remedy against a supervisory authority and a right to an effective judicial remedy against a controller or a processor as well as the right to compensation from Article 82 of the GDPR potentially bringing about lawsuits with damages far exceeding much discussed administrative fines. [18]

VIII. Conclusion

The new EU legal framework of data protection has already been percieved, especially outside of the Union, as strict, creating additional administrative overhead and numerous new obligations for data controllers especially concerning appropriate technical and organisational protection measures.

From the perspective of research institutions, libraries and archives however, the new Regulation creates exemptions and opportunities to reuse personal data potentially facilitating vibrant landscape of secondary use of collected personal data.

Personal data has become a vital digital asset and resource, and the EU lawmakers hope the new Regulation will foster research and development of new innovative services and products.

In order to make use of this provisions, as well as to fulfill obligations set by the GDPR, research institutions and other organizations need to assess their personal data use. In practice, this means they need to create and regularly update records of processing, review their organisational and technical protection measures and conduct other activities mandated by the Regulation.

If their activities meet the Regulation criteria regarding mandatory designation of data protection officers, they need to carefully choose and appoint experts with appropriate skills.

Regulating limitations of users rights, especially concerning the retention of data and allowing processing for secondary use new provisions may allow researchers to process and use data that would have been legally inacessible in the current framework, enabling the development of new information society services and products as well as fostering more efficient research.

At this point, it remains somewhat unclear on how exactly will the limitations and exceptions regarding secondary use of research data containing personal data look from the perspective of organizations established in different Member States after they adopt companion national legislation.

References

[1] Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), Official Journal of the European Union, L 119/1.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050

[3] Treaty on European Union and the Treaty on the Functioning of the European Union, Official Journal C 326, 26/10/2012 P. 0001 - 0390

[4] Charter of the Fundamental Rights of the European Union, 2012/C 326/02, Official Journal of the European Union, C 326/391

[5] Latham&Watkins, The General Data Protection Regulation (GDPR) National Implementation Tracker, available at https://www.lw.com/admin/Upload/Documents/LW-FINAL-GDPR-National-Implementation-Tracker-Feb2018.pdf

[6] Article 2. (a) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050

[7] Personal Data Protection Act, OG of the Republic of Croatia 103/03, 118/06, 41/08, 130/11, 106/12.

[8] Recital 53 of 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), Official Journal of the European Union, L 119/1.

[9] Article 5.1.f of 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), Official Journal of the European Union, L 119/1.

[10] Andress, J.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress, 2014.

[11] Rumbold, J.M.M., Pierscionek, B.: The Effect of the GDPR on Medical Research, Journal of Medical Internet Research, 2017 Feb; 19(2): e47.

[12] Article 7 and Recital 52 of 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), Official Journal of the European Union, L 119/1.

[13] Maldoff, G: The Risk-Based Approach in the GDPR: Interpretation and Implications, IAPP 2017. Available at: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf

[14] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev.01 available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[15] WP29 DPIA Guidelines, p. 11., available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[16] Articles 37 and 39 of 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), Official Journal of the European Union, L 119/1.

[17] Rydén, J.: Memo: Case Study – Data Protection Reform, available at: http://www.eblida.org/Experts%20Groups%20papers/EGIL-papers/EGIL_Data_Protection_Regulation_Memo_CaseStudy_2016.pdf

[18] Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law (2013/396/EU), Official Journal of the European Union, L 201/60.