Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance

Katulić, Tihomir; Katulić, Anita

Submitted on: 25.06.2019

IFLA CPDWL Satellite meeting:
Librarians and information professionals as (pro)motors of change:
immersing, including and initiating digital transformation for smart societies
Date: 20 – 21 August 2019
Location: National and University Library in Zagreb, Croatia

Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance

Tihomir Katulić
Faculty of Law University of Zagreb, Croatia.
tkatulic@pravo.hr

Anita Katulić
National and University Library in Zagreb, Croatia.
akatulic@nsk.hr

Abstract:

The General Data Protection Regulation that recently entered into force in the European Union represents a significant milestone in development of efficient personal data protection in Europe. As a substantial upgrade to current legal framework it now explicitely provides the rights and freedoms of data subjects and responsibilities of data controllers and data processors. The Regulation is directly applied in legal systems of Member States and contains provisions designed to ensure data controllers, such as libraries, process personal data in line with the recognized principles of data protection.
Libraries acquire personal data of users, authors and other physical persons (data subjects) through different means. Recognizing the need for specialized oversight and guidance on implementing Regulation mechanisms to ensure safe and secure personal data processing, the new law extensively regulate the position, role and competence of data protection officer whose main tasks include providing compliance advice for data controllers, handling of user requests and contact with the competent national data protection authority.
As most libraries fall under the category of public bodies or authorites, the law mandates designation of such individual. Even when this is not the case and other Regulation conditions do not apply, it may be prudent to designate a data protection officer out of concern for data subject rights and freedoms and to coordinate efforts to achieve the highest level of compliance.
The purpose of this presentation is to point out difficulties in achieving compliance for libraries in the public sector, identify the issues where having a data protection officer might be useful, help libraries establish a DPO position and choose a person of adequate competence.

Keywords: Data Protection Officer, Libraries, Personal Data Protection

Introduction

The General Data Protection Regulation that recently entered into force in the European Union represents a significant milestone in development of efficient personal data protection in Europe.

As a substantial upgrade to previous legal framework it now explicitly provides the rights and freedoms of data subjects and responsibilities of data controllers and data processors. The Regulation is directly applied in legal systems of Member States and contains provisions designed to ensure data controllers, such as libraries, process personal data in line with the recognized principles of data protection. The impact of the Regulation is far wider than just the data controller and processor operations in the EU. As was the case with the 1995 Data Protection Directive, the new Regulation is positively impacting the development of personal data protection as a fundamental right in legal systems far from Europe and the EU.

Libraries, their associations, information services providers and related national and international public registers acquire personal data of users, authors and other physical persons (data subjects) through different means and in different roles from the perspective of the Regulation. All these institutions however need to collect and process personal data in accordance with the regulated legal basis of processing, prepare to support and respond to their users when exercising their rights, apply appropriate technical and organizational protection measures, identify, treat and respond to risks for data subject rights and freedoms and finally cooperate should a personal data breach occur.

Recognizing the need for specialized oversight and guidance on implementing Regulation mechanisms to ensure safe and secure personal data processing, the new European legal framework of data protection extensively regulates the position, role and competence of data protection officers, data protection experts whose main tasks include providing compliance advice for data controllers, establishing organizational information security measures, measuring and reviewing activities aimed at handling of user requests and contacts with the competent national data protection authorities.

As most libraries fall under the category of public bodies or authorities, the law mandates designation of such individual. Even when this is not the case and other Regulation conditions do not apply, it may be prudent to designate a data protection officer out of concern for data subject rights and freedoms and to coordinate efforts to achieve the highest level of compliance. The purpose of this paper is to point out difficulties in achieving compliance for libraries in the public sector, identify the issues where having a data protection officer might be useful, help libraries establish a DPO position and choose a person of adequate competence.

Libraries and personal data

Libraries all over the world are spearheading the digital transformation of public bodies in order to satisfy the needs of the advancing information society. The digital trace library users leave when using library services allows for better recognition of the library patron needs, whoever, these activities leave substantial amounts of personal information present in the library information systems.

According to the GDPR principle of accountability, the libraries as data controllers need to ensure safe and secure processing of personal data in accordance with the GDPR principles of data processing, established legal basis of processing and the rights of data subjects.

Since libraries collect data through various channels, from library patrons through filling out formes to register for the use of the library, through library information systems, search histories and access to contents to library web services, interchange services and event attendance, the basis of compliance effort will usually be to identify proper legal basis for processing and fill out the records of processing activity as mandated by the Article 30 of the Regulation.

Libraries collect personal data not only about their users, but also managing legal deposits collections and the web harvesting material which may involve the processing of sensitive personal data. Since personal data in cases such as web harvesting will be processed for purposes other than those for which the personal data were initially collected and should according to Recital 50 of GDPR be allowed only where the processing is compatible with the purposes for which the personal data were initially collected, additional national legislation will also have a role in bridging this secondary use legality gap.[1]

Managing authority files in library catalogues also falls under GDPR and libraries should care about transparency concerning data subjects rights to be informed about their personal data processing and provide suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[2]

Regarding to specific measures libraries should implement appropriate technical and organizational measures for ensuring that only personal data which necessary for each specific purpose of the processing is processed. Since the sensitive personal data should not be processed, unless processing is allowed in specific cases set out in the Regulation, Member States law may lay down specific provisions on data protection for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. These provisions should be enacted in national laws accompanying the Regulation, such as the Croatian Law on Application of the General Data Protection Regulation.[3]

Every library should prepare records of processing activities as mandated by the Article 30 of the Regulation outlining the purpose for using personal data, the categories of personal data, time limits for processing and technical and organizational measures used to protect personal data. Establishing legal basis for every category of personal data processed in library and employing "*privacy by design*" principles mapping out current processes relating to personal data, also when introducing new processes involves evaluating how this will impact on the personal data that library collects and processes. If relying on consent for processing of personal

[1] Rydén J. Memo/Case study – data protection reform, p.17 [2019-06-18] Available at: http://www.eblida.org/Experts%20Groups%20papers/EGILpapers/EGIL_Data_Protection_Regulation_Memo_CaseStudy_2016.pdf

[2] See: Katulić, A. Normativna baza imena u kontekstu Opće Uredbe o zaštiti podataka. // Vjesnik bibliotekara Hrvatske 61, 1(2018) , 573-592. doi:10.30754/vbh.61.1.599 [2019-06-18] Available at: https://www.hkdrustvo.hr/vjesnik-bibliotekara-hrvatske/index.php/vbh/article/view/599

[3] Law on Application of the General Data Protection Regulation, OG of the Republic of Croatia no. 42/2018.

data, libraries should ensure that terms and conditions that relate to using patrons' personal data are easily accessible and must be able to demonstrate that the consent is freely given to library.[4]

In general, regarding privacy, librarians have been guided by the IFLA Code of Ethics that identifies respect for personal privacy and data protection in the relationship between user and library as core principle.[5]

IFLA's Statement on Privacy in the Library Environment contains privacy-related recommendations for libraries that indicate which principles should be used in library operations to raise user awareness of personal data protection and introduce safety measures within the library and information system. These recommendations include respecting and advancing privacy at the practical level and as a principle, raising awareness among users about the implications of processing activities, use of their data and providing guidance in data and privacy protection.

Since service providers used by libraries may collect data on users' activities, communications and transactions and cloud-based library systems may transfer and store users' data outside of library or information system, maintaining users' privacy may face serious challenges. Therefore libraries should take measures to limit collection of personal data about their users and the services that they use in accordance with the principle of purpose limitation and data minimization as enshrined by the Regulation. [6]

GDPR compliance process in library usually covers several phases: appointing a team of experts in the fields of legal, IT and security compliance to perform the GDPR compliance process; project setup and raising awareness within the library on key GDPR aspects, requirements and needs through education materials and privacy policies; maintaining a record of processing activities under article 30 of GDPR; conducting privacy impact assessments, identifying compliance gaps and regulating the position and responsibilities of the data protection officer.[7] Finally, identifying any third party data processors and reviewing contracts with vendors will be required to ensure adequate security is in place.

From a human resources perspective, while being custodians of access to large databases and serving a large number of patrons, libraries are usually not well equipped to deal with changing compliance requirements rarely employing experts in the field of data protection and information security.

At the same time, the number of users, the volume of personal data and their status usually as public bodies in case of libraries will usually demand the designation of a data protection officer.

---

[4] See: White, B. Briefing: Impact of the General Data Protection Regulation 2018., p.2-3 [2019-06-13]. Available at: https://www.ifla.org/files/assets/clm/publications/briefing_general_data_protection_regulation_2018.pdf

[5] IFLA Code of ethics [2019-06-18] Available at: https://www.ifla.org/publications/node/11092

[6] IFLA Statement on Privacy in the Library Environment [2019-06-18] Available at: https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf

[7] Papaioannou, G.; I. Sarakinos. The General Data Protection Regulation (GDPR, 2016/679/EE) and the (Big) Personal Data in Cultural Institutions: Thoughts on the GDPR Compliance Process // Maturity and Innovation in Digital Libraries, 20th International Conference on Asia-Pacific Digital Libraries, ICADL 2018, Hamilton, New Zealand, November 19-22, 2018, Proceedings / ed. by Milena Dobreva, Annika Hinze, Maja Žumer. Heidelberg: Springer International Publishing, 2018.

Such individual can be an employee of the library or contracted through a service contract. In any case, the DPO has to posess certain qualifications, experience. The GDPR provides that a DPO has to be designated on the basis of professional qualities, especially expert knowledge of data protection law and practices and the ability to fulfil the tasks from Article 39 of the Regulation, which we will discuss in more detail *infra*.

Designation, position and tasks of the data protection officer data protection law

While the 1995 Data Protection Directive did not explicitely regulate the data protection officer[8], this position is not unknown to data protection laws in EU Member States. National data protection laws in Germany, for example, adopted the data protection officer provisions as early as late 1970's. From there, these provisions spread to legal systems of many EU Member States, especially in the first decade of the twenty first century.

While many of the Member States introduced data protection officers as an institute of their national data protection laws, in practice most of the national laws did not adequately regulate their designation, position or competences, usually satisfied to regulate their tasks profiling their position as administrative and advisory.

The designation criteria, such as one found in Croatian Personal Data Protection Act, was quantitative in nature, mandating the designation of the data protection officer on the basis of criteria of a data controller employing a certain number of employees did not take into account the nature, scope and a volume of personal data processing done by the data controller.

This led to unacceptable situations where data controllers conducting processing involving sensitive categories of data such as data related to health, political views, religion or ethnicity would not be obliged to designate a data protection officer unless employing at least 20 or a similar number of employees.

With this in mind, the General Data Protection Regulation in Articles 37, 38 and 39 extensively regulates the designation, position, skillset and tasks of the data protection officer.

Instead of a quantitative criteria, the data controller will now have to appoint a data protection officer if his processing activities and his status meet qualitative criteria related to the nature, scope and volume of processing.
If a data controller is a public authority or body, and a large number of public libraries meet this criteria according to the definition of public authorities or bodies in EU Member States' legal systems, then they are required to appoint a data protection officers.

Even libraries who do not fall under the definition of a public authority or body will have to appoint the DPO should they conduct data processing activities that consist of regular and systematic monitoring of data subjects on a large scale, should they contain a large scale processing of special categories of data as defined by the Article 9 of the Regulation etc.

While it can be said that there is an increase in the level of accountability of the data controller provided by GDPR provisions such as higher penalties and mandatory breach reporting, data protection impact assessment is also an important tool for demonstrating accountability. Data

[8] 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

protection officer who has suitable knowledge in data protection will be a key person to assist DPIA. [9]

Role of the DPO in libraries

The General Data Protection Regulation details the position and the tasks of the data protection officer in line with the principles of processing, especially from the perspective of risk managament and information security.[10]

The tasks of the DPO include providing advice to controllers and processors and the employees carrying out personal data processing tasks. In the context of libraries, this means that designated data protection officers need to be able to advise the management of the library, its partners including information services providers and institutions receiving data from libraries as well as library employees who conduct day to day operations which involve library patrons' personal data.

Further, the data protection officers are tasked with monitoring the compliance of their organization with the GDPR, other EU and national legislation as well as the policies of the data controller or processor.

This provision demands that data protection officers participate in awareness raising efforts, organize and/or lead training of library employees, conduct audits to measure the compliance with data protection law as well as library's own policies and procedures.

DPOs additionally have an obligation to participate and contribute to data protection impact assessments and monitor their results and if needed, consult with the supervisory authority.
Finally, should a personal data breach occur, the DPO acts as a contact point for the data subjects and the supervisory authority.

Regarding the resources required for data protection officers, the Regulation mandates that data controllers or data processors provide necessary resources to data protection officers necessary to carry out their tasks.

The organization, in this case a library, therefore needs to set aside financial and organizational resources to support the work of the data protection officer, as well as help him or her maintain their expertise and skillset to stay in touch with developments in this quickly evolving regulatory field.[11]

In practice, this means that the library management should actively support the DPO and allow them sufficient time to fulfil their duties especially if they have been designated from the ranks of library employees already carrying out other duties and tasks. The Article 29 Working Party Guidelines on Data Protection Officers published in 2016 in this regard recommend.

Designating a competent data protection officer

[9] See: Katulić, A.; Katulić, T. GDPR and the Reuse of Personal Data in Scientific Research // MIPRO 2018 : 41st International Convention Proceedings, p.1514-1519

[10] 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), Article 39

[11] WP29 Guidelines on Data Protection Officers, WP243 16/EN published on 13th of December, 2016, p. 13

While the Regulation does not the define the required level of expertise, it is apparent from the Guidelines document that the level of expertise has to be proportional to the complexity and the amount of personal data processed by the organization.

Additional factors apply such as if an organization systematically transfers personal data outside of the European Union, or only occasionally or if personal data recognized as special (sensitive) category of data is being collected and processed.

In the context of library operations, as well as in any other sector, a thorough understanding of the rules and operations of modern libraries is required. Since the DPO is expected to audit and help implement risk management practices and observe the compliance of the library with the data protection rules, knowledge on the relevant operations and processes as well as administrative rules of the organization is a necessary precondition.[12]

DPO role in ensuring the observance of data protection principles, data subject rights and freedoms is vital so from a personal character perspective, a data protection officer should posses a high level of personal integrity and professional ethics, a requirement obvious even in the previous legal framework.[13]

Unlike the previous legal framework which did not forsee a designation of an outside DPO, the Regulation now explicitely allows a designation of a data protection officer not currently employed by the data controller. DPO can now be outsourced and contracted through a service contract.

As we have already mentioned, taking into account the provisions of the GDPR regarding adequate expertise and skillset required for the position of the DPO, many libraries will face a challenge in identifying such individuals among their work force. Instead, some may turn to the rapidly developing market for DPO services.

Position of the DPO

Within an organization, data protection officers ought to be able to perform their duties with a sufficient level of independence from the organization. In practice, this means that the management of a library as a data controller is not in a position to give instructions, prioritize or direct the designated data protection officer in performance of his job.

Since the Regulation demands that data controllers and data processors process personal data with data protection principles in mind, especially the principle of accountability, should a situation arise where the management has different opinion on the risk of processing, implementation of adequate technical or organizational security measures or any other issue that relates to data protection and potentially rights and freedoms of data subject, a DPO should

[12] Ibid, p.11

[13] Such as in the provisions of the Croatian Personal Data Protection Act which, in Article 18.a prohibits designating as DPO:"... A person against whom the process for the violation of duty ex officio or obligations is conducted, or on whom the sanction for the violation of duty ex officio or obligations was imposed, or on whom the sanction for the violation of the code of ethics or other rules of conduct prescribed by the employer was pronounced, shall not be appointed as a personal data protection official."

be allowed to voice his concerns directly to library management. Likewise, a DPO should not be dismissed or penalised by the data controller or processor for performing his tasks.[14]

Conflict of Interest

Organizations such as libraries may not have sufficient resources to designate an employee DPO in a way that data protection is his only function in a library. Instead, often will be the case that such employees have other duties and tasks to perform.

These other duties may interfere with DPO's ability to perform data protection tasks in line with the General Data Protection Regulation. Whether this is the case is specific to the structure of each organization. The WP29 Guidelines recommend that each organization that has an obligation to name a DPO should identify employee positions incompatible with a DPO function, create rules to avoid conflict of interest etc. In general, if an employee participates in decisions regarding the nature and purpose of processing, those positions should be considered as positions with a conflict of interest with a DPO and these employees would not be able to perform as independent and objective data protection officers.

Conclusion

In this paper we tried to outline the reasons why many public libraries will need to designate a data protection officer, mostly on the basis of the fact that public libraries which are established as independent institutions fall under the category of a public body, but also on the basis of the quality and quantity of their processing of personal data.

Since libraries in general do not employ people with adequate skills in data protection and information security to satisfy GDPR DPO requirements, outsourcing may be necessary. Public library founders, usually units of local and regional administration will need to include the cost of hiring these professionals or establish DPO offices to serve libraries and other public institutions in their area.

Larger institutions may find suitable employees to be designated as data protection officers. Those that do will need to carry out a conflict of interest probe when establishing the position and tasks of the DPO designated from the employee ranks.

One of the major challenges for library DPOs will be to conduct risk analysis and data protection impact assessments for personal data processing done in libraries.

The application of the GDPR and the new generation of national application laws poses significant questions against any export of personal data to countries whose legal systems do not offer the recognized level of personal data protection. In this regard, a review of global personal data processing activities in the context of library operations needs to be conducted. Additionally, decisions in proceedings before the European Court of Justice on the validity of export instruments such as the standard contractual clauses and specific adequacy decisions such as the EU US Privacy Shield will have an impact.

[14] General Data Protection Regulation, Article 38.3

To conclude, data controllers in the culture and education sectors need additional resources to effectively complete compliance projects, especially to ascertain risks from available information systems and infrastructure. The new data protection standards of the EU are going to have a far reaching impact on the development of personal data protection and will affect library operations worldwide.

References

Article 29 Working Party Guidelines on Data Protection Officers, 16/EN W243 from 13th of December, 2016. [2019-06-21] Available at: 2https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

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

IFLA Code of ethics [2019-06-18] Available at: https://www.ifla.org/publications/node/11092

IFLA Statement on Privacy in the Library Environment [2019-06-18] Available at: https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf

Katulić, A. Normativna baza imena u kontekstu Opće Uredbe o zaštiti podataka. // Vjesnik bibliotekara Hrvatske 61, 1(2018) , 573-592. doi:10.30754/vbh.61.1.599

Katulić, A.; Katulić, T. GDPR and the Reuse of Personal Data in Scientific Research // MIPRO 2018 : 41st International Convention Proceedings, 1514-1519

Papaioannou, G.; I. Sarakinos. The General Data Protection Regulation (GDPR, 2016/679/EE) and the (Big) Personal Data in Cultural Institutions: Thoughts on the GDPR Compliance Process // Maturity and Innovation in Digital Libraries, 20th International Conference on Asia-Pacific Digital Libraries, ICADL 2018, Hamilton, New Zealand, November 19-22, 2018, Proceedings / ed. by Milena Dobreva, Annika Hinze, Maja Žumer. Heidelberg: Springer International Publishing, 2018.

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) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 [2019-06-13] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=HR

Zakon o zaštiti osobnih podataka // pročišćeni tekst, Narodne Novine 103/03, 118/06, 41/08, 130/11, 106/12 Available at: https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka

Law on Application of the General Data Protection Regulation, OG of the Republic of Croatia no. 42/2018. / Zakon o provedbi Opće uredbe o zaštiti podataka. // Narodne novine 42, 805(2018). [2019-06-13]. Available at: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

White, B. Briefing: Impact of the General Data Protection Regulation 2018. [2019-06-13]. Available at: https://www.ifla.org/files/assets/clm/publications/briefing_general_data_protection_regulation_2018.pdf

Rydén J. Memo/Case study – data protection reform [2019-06-13] Available at: http://www.eblida.org/Experts%20Groups%20papers/EGIL-papers/EGIL_Data_Protection_Regulation_Memo_CaseStudy_2016.pdf