Application of the principle of transparency in processing of European national libraries patrons' personal data

Katulić, Anita; Katulić, Tihomir; Hebrang Grgić, Ivana

Application of the principle of transparency in processing of European national libraries patrons' personal data

Anita Katulić
National and University Library in Zagreb, Zagreb, Croatia
Tihomir Katulić
Faculty of Law, University of Zagreb, Zagreb, Croatia, and
Ivana Hebrang Grgić
Faculty of Humanities and Social Sciences, University of Zagreb, Zagreb, Croatia

Received 17 November 2021
Revised 22 January 2022
30 January 2022
Accepted 2 February 2022

Abstract

Purpose – The purpose of this paper is to examine the relationship between the legal obligation of European libraries to ensure the transparent personal data processing and respect for user privacy. This paper will examine how libraries use privacy notices on websites to communicate with patrons about the processing of personal data and in what manner have libraries been guided by applicable transparency guidelines.

Design/methodology/approach – The method used is the analysis of privacy policies and other privacy documents found on the websites of national libraries. The analysis sample includes documents of 45 European national libraries, 28 out of those being national libraries of European Union (EU) Member States. The elements for this analysis are derived from the mandatory elements of the General Data Protection Regulation and the recommendations of the WP29/EDPB Transparency Guidelines.

Findings – The findings suggest that European national libraries largely adhere to EU data protection standards. In total, 60% libraries use a separate privacy page, and 53% of the EU Member State national libraries websites managed to comply with publishing all necessary data protection information in a way recommended by the Guidelines, compared to 47% of non-Member State national libraries.

Originality/value – The research contributes to the understanding of the importance of the principle of transparency and its operationalization.

Keywords Data protection, Personal data, Library privacy, Patron privacy, National libraries, Principle of transparency

Paper type Research paper

Introduction

For the most part of the 20th century, libraries did not rely on computer programs for their everyday activities. Library loans were recorded by hand on paper and entered into borrowing cards and pockets for each user (Pedley, 2020, pp. 2–3). This way, the card from the book borrowed by the user was inserted into the pocket in the user box, and upon return, the card would be returned to the pocket in the book. After the book was returned, there was no record of the individual user's borrowing history. Even in such cases there were certain privacy risks, for example in case of theft or loss of the user's loan pocket as there was no backup version (*backup*). Furthermore, the data could not be accessed from other places, but could only be accessed by individual librarians behind a particular library desk.

Digital Library Perspectives
© Emerald Publishing Limited
2059-5816
DOI 10.1108/DLP-11-2021-0097

Traditional libraries and digital libraries differ in the scope of personal data they process (Iglezakis, 2011, p. 414). The basic data that libraries of all types process are records of members, borrowing history, reservations and other activities that arise based on the user's activity and use of services. Modern digital libraries also process data on the use of interlibrary loan services, electronic sources, data of users who use online and interactive services, e-mail addresses, Web forms and search history on the computer for library users. Data on financial transactions of users, debts, etc. are also recorded in computer library systems.

Libraries are no longer just spaces that users come to but also continuously available online services and are increasingly being used remotely. For such services, libraries use a variety of service intermediaries, such as *cloud* services, e-resources, data analytics companies and e-lending. Libraries also use surveillance camera systems in their space. Also, the design of many library 2.0 services capitalize on access to patron information and might require additional tracking, collection and aggregation of patron activities (Zimmer, 2013). For these reasons, the issue of protection of personal data of users as well as the protection of their privacy and confidentiality in general is more challenging today to adequately address than it was in the past (Gorman, 2015, p. 191). Libraries today need to make greater efforts to secure and preserve a relationship based on trust than libraries in the past.

Literature review

Library as a place of safe access to information

The relationship between the library and the user is traditionally based on trust and confidentiality of data. Ethical principles of the library profession are set out in documents such as the *IFLA Code of Ethics* and include guidance on the promotion of ethical use of information, respect for privacy and protection of personal data that must be exchanged between the library and the user (*IFLA Code of Ethics for Librarians and Other Information Professionals*, 2012, pp. 2–3).

As libraries enable people to take advantage of the opportunities offered by information and communication technology, provide support and training for media use and information literacy development, and protect users' rights to access information in a secure environment (*IFLA Statement on Libraries and Development*, 2013), to ensure free access to information, the users should be confident that the information requested through library services will be searched for in a secure environment and that the data about them or the information they requested will not be disclosed.

Caldwell-Stone points out that privacy is particularly important in relation to the intellectual freedom that libraries advocate as public institutions, as "a lack of privacy in what one reads and views in the library can have a significant *chilling effect* upon library users' willingness to exercise their [. . .] right to read "(Caldwell-Stone, 2015, p. 184). In other words, the risk of disclosure of personal data or of being under surveillance implies an undesirable slowing or discouragement in searching new or unpopular topics. Richards links the *chilling effect* to intellectual freedom because the knowledge or awareness that someone is monitoring what information we seek, read and research negatively affects the fundamental individual interests of individuals such as personal freedom, intellectual privacy, autonomy, and self-development. Intellectual privacy is essential for a culture of freedom of expression (Richards, 2015, pp. 95–108). Richards presented intellectual privacy as a type of privacy and described it as "protection of records of our intellectual activities" where "the ability to freely decide and develop new ideas depends on a significant degree of intellectual privacy" (Richards, 2008, p. 389).

Librarians have an important role to play in educating users about privacy: they can offer source materials, establish information centers and organize events where citizens can learn about security in an online environment. In this way, they can fulfill their obligation to provide access to information and enable citizens to choose how to use their personal data when using online services. In recent years, manuals and guides on ensuring privacy and promotion of user data protection rights have been prepared by librarians in Europe and the idea has spread that libraries must ensure that they truly do everything to protect personal data within their systems and internal processes (Charillon *et al.*, 2018, p. 4).

It is important to be aware that each of the activities of users of library services, electronic resources and publisher platforms to which the library provides access also entail certain risks of data misuse and data processing for purposes the user has not been informed about. As part of the role of lifelong learning providers, the library should provide all the necessary information on the processing of personal data of users in relation to service providers (controllers of personal data processing). According to *IFLA Statement on Privacy in the Library Environment*, each library decides which data to process, how long to keep it, negotiates with service providers about the terms and protection of personal data, may refuse or restrict services that collect excessive data or compromise user privacy (*IFLA Statement on Privacy in the Library Environment*, 2015, p. 2).

While all data protection principles enshrined by the General Data Protection Regulation (GDPR) are equally important and must be reflected in the handling of personal data in the institution, the principle of transparency, which will be discussed below, presents a unique opportunity to establish a relationship of confidentiality between the library and users.

The right to privacy and the right to the protection of personal data

Let us for a moment examine the difference between the right to privacy and the right to protection of personal data to determine the basis for reducing the risk to the privacy of library users. The right to privacy and the right to the protection of personal data are often perceived as synonyms, as aspects of the same right. However, in modern European legislation they unequivocally exist as two separate and equally valuable rights, as seen in the EU Charter of Fundamental Rights (EU Charter of Fundamental Rights, 2016, Articles 7 and 8).

Privacy is a complex category that has changed throughout history and depending on the degree of social development and democratic processes within countries. The right to privacy was internationally recognized by the 1948 Universal Declaration of Human Rights. In general, privacy can be divided into multiple aspects or aspects depending on several factors such as time, environment and context. Koops *et al.* (2016, pp. 566–569) distinguish nine types of privacy: bodily, intellectual, spatial, decisional, communicational, associational, proprietary, behavioral privacy and ninth – informational privacy that overlaps with all eight types. Informational privacy occupies a special place and represents a point of contact with other types of privacy for the reason that it relates to the collection and dissemination of data, and includes rules for the management, collection and use of personal data. Informational privacy generally includes control over the dissemination of personal data and control over access to personal data.

The right to protection of personal data in Europe was widely recognized as a separate right (Gonzalez Fuster, 2014, p. 175) and separate from the right to privacy in 1981 when the Convention 108 on the Protection of Individuals With Regard to Automatic Processing of Personal Data was adopted by the Council of Europe. The basic principles of personal data protection set out in Convention 108 have evolved to date, and the personal data protection framework of the European Union (EU) in the Data Protection Directive of 1995 has been

greatly expanded and upgraded with the entry into force of the 2016 GDPR. As the GDPR adopted more detailed obligations for personal data controllers, its application was accompanied by a two-year grace period and an increasing number of guidelines by bodies such as the Article 29 Working Party and later by the European Data Protection Board to facilitate easier interpretation and implementation of the new Regulation. The reason for this relatively long period of adjustment to the new legal framework lies in the fact that such a framework brings many innovations that have an impact on the operations of institutions, such as access to personal data management based on risk assessment, extension of personal rights and sanctions (Lambert, 2018, p. 102).

The basic principles of personal data processing require that any processing of personal data should be lawful and fair, and personal data should be appropriate, relevant and limited to what is necessary for the purposes for which are processed and up-to-date. The period during which personal data are processed should be as short as possible. The Regulation demands that data subjects are given adequate information on how and to what extent their data are processed, and what are the risks, rules, safeguards and rights of individuals related to the processing of personal data, which is directly related to the rights of individuals whose personal data are processed. For this reason, the principle of transparency is the focus of the research and we will return to it below.

Prior to the entry into force of the GDPR, only a few studies were conducted in Europe concerning library privacy policies. As mentioned earlier, the GDPR was preceded by the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive). The directive was to be implemented in the legal systems of the Member States by 1998.

In the field of librarianship, Noh (2017) classifies the literature on library privacy into five categories: studies on the concept of privacy, studies on privacy awareness, studies on privacy infringement, studies on privacy policies and studies on customized services and privacy.

One of the surveys was conducted in 2003 in academic and special libraries in the UK during the *Privacy in the Digital Environment project* which showed that privacy is not high on librarians' priorities, only 14% of libraries had privacy notices and 64% had data protection policies in place (Sturges *et al.*, 2003, pp. 44–50).

A survey conducted in Croatian and Dutch public, special and academic libraries in 2007, after the entry into force of the Data Protection Directive (the Republic of Croatia adopted the Personal Data Protection Act in 2003) concluded, among other things, that libraries mostly overlooked the communication aspect in processing personal data with users even when they have regulated privacy policies or personal data protection policies (Schepmann *et al.*, 2008).

Ahead of the entry into force of the GDPR, a UK survey on the level of library readiness for GDPR implementation showed an improvement over the survey conducted nine years earlier, librarians' awareness of the new legal framework and several key aspects. However, librarians still participate very little in the organization of personal data protection management, and 48% do not know if they have a privacy policy in the library although 85% of them consider this topic to be extremely important (Bailey, 2018).

The principle of transparency in the processing of personal data of library users and privacy notices

Transparency, as a principle in data protection, is a feature that in European Union law that refers to building trust in processing activities that affect individuals (data subjects)

allowing them to understand and, if necessary, challenge these processing activities (*Handbook on European Data Protection Law*, 2020, p. 117).

In the context of personal data protection, it is also an expression of the principle of fairness of personal data processing set out in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR Article 5(1)a, transparency is now one of the fundamental principles of personal data protection and is essentially linked to legality and fairness as a principle of processing and the new principle of liability under the GDPR.

Transparency of processing *vis-à-vis* data subjects means that it should be transparent to individuals how personal data relating to them are collected, used, made available or otherwise processed, and to what extent that personal data is or will be processed, including information on retention periods and data transfer to other executors or controllers. In addition, any information regarding the processing of personal data is required to be easily accessible and understandable and to use clear and simple language, especially if the information is intended for children. Individuals should be informed about the risks of processing their personal data, the rules of data processing and protection, or the protection measures taken (GDPR, Recital 39).

Another novelty and consequence of the application of the European regulation as a legal instrument of harmonization of European legislation in the field of personal data protection is the application of GDPR in a limited extraterritorial sense in relation to controllers who are not based in the European Union but process personal data of individuals in the EU Member States or offer products and services in the common European market (*Guidelines of the European Data Protection Board 3/2018 on the territorial application of the GDPR*, 2018, p. 5).

The GDPR significantly extends the scope of European data protection rules to controllers established and established outside the Union if they process respondents' personal data in the Union for the purpose of offering goods or services to respondents (including free services) or monitoring their conduct (EDPB Guidelines 3/2018 on the territorial application of GDPR, 2018, p. 12). National libraries are open for membership to users from all over the world, of course, each library on its own terms. Thus, the libraries of non-EU countries will also process data from users belonging to the EU, and these rules will also apply to them. Libraries should provide information to their users about the collection and processing conditions of their data.

Information about processing of personal data published by the data controller, in our case libraries, is called a Privacy Notice, Personal Data Protection Notice or sometimes a Privacy Statement or Privacy Policy. *The WP29 Transparency Guidelines* (*Article 29 Working Party Guidelines*) can serve as a guide for understanding and drafting privacy notices. The Guidelines state that in case that the controller (i.e. the library) has its own website, the personal data protection notice should be published in "layered form" on the website (Article 29 Data Protection Working Party, 2018, p. 14). The layered view or format is clarified and, according to the *Transparency Guidelines*, means a form of the privacy notice that visually offers direct access to the part or section of the privacy notice of interest to the user, without making the effort to search large amounts of text.

As the notices are intended for the end user, they should be concise and easily accessible under the *Transparency Guidelines*, which is further clarified in the *Guidelines*: these notices should be clearly distinguished from other non-privacy information such as general terms and conditions of service use (e.g. regulations on the use of library services and materials), and it should be possible to provide links to the various categories of information that must be provided to the respondent, instead of all this information being displayed in a single notice on the screen.

In addition, the graphical design of the first layer of the notice should allow a clear overview of all available information on processing as well as on where and how it can find

detailed information within the layers of the privacy notice. It is also important that the information contained within the different layers of the notification is consistent and that conflicting information is not provided in these layers (*Article 29 Working Party Guidelines*, 2018, p. 7, 19). This way, the presentation of information relevant to the library users is more adapted to the internet environment.

In addition to the layered privacy notice in the digital environment, users should also have access to all information in one place or in one complete document (digital or paper) if they wish to gain insight into all the information intended for them (*Article 29 Working Party Guidelines*, 2018, p. 11).

The new legal framework established by the GDPR for data subjects potentially allows for greater control over the processing of their personal data. It is the principle of transparency, or the application of that principle in relevant provisions, that enables data subjects to gain easier insight into the procedures of personal data processing and, based on that and the principle of accountability, to hold the controllers and processors accountable for their handling of personal data.

The principles of personal data processing enable the exercise of data subjects' rights such as withdrawal of consent or the right to access their personal information (Voigt and von dem Bussche, 2017, p. 142). Mandatory information to be provided to the data subject by the controller is set out in Articles 12 to 14 of the GDPR, and includes the following:

- identity and contact details of the data controller;
- contact details of the data protection officer;
- predetermined purposes of processing for which personal data are used as well as the legal basis for processing; and
- recipients or categories of recipients of personal data.

Article 12 of the GDPR sets out the general rules to be followed to meet the principle of transparency. The general rules apply to: providing information to respondents whether the personal data were obtained from respondents or from other sources (Articles 13 to 14 of the GDPR), which specify the scope of information that must be provided to respondents. Other rules refer to informing the respondents about the exercise of their rights (from Articles 15 to 22 of the GDPR).

Aim and methods of research

The survey was conducted in January 2022. The aim of the research is to investigate the extent to which recommendations for transparency have been implemented in the privacy notices of European national libraries, whether libraries have been guided by the Transparency Guidelines and whether there is a difference in transparency between EU and non-EU libraries. The analysis of the results aims to find out whether the obligations in the form of regulations and accompanying guidelines and instructions on the transparency of the processing of personal data of national libraries in Europe are related.

The research questions we wanted to answer in the research are:

RQ1. How and in what manner do national libraries use privacy notices to communicate with users about the processing of personal data?

RQ2. To what extent have national libraries in Europe relied on the Article 29 Working Party Transparency Guidelines?

RQ3. To what extent do libraries state the purposes and legal bases for all processing of personal data in the notices?

The methods of data collection used are:

- the identification of national library's website and the relevant documents of the national libraries of each country in Europe via the Google search engine by entering the name of the country and the term in English "national library";
- search for the term "cookies" [1] on the library's website;
- search for the terms "privacy", "privacy policy" and "data protection/personal data protection";
- search for regulations on the use of services and materials; and
- search for the terms "personal data" on the library's website in English, as well as the official language of every Member State.

If the requested privacy information pages were found, an analysis of the content of the documents found was performed. Criteria for analysis are derived from GDPR Art. 12 and the Transparency Guideline. Thus, it was investigated:

(1) the existence of privacy information separate from other information or policies (such as a separate privacy policy, service policy, etc.);

(2) the "stratification" (layered form) of the privacy notice as described in the Guidelines; and

(3) the existence of mandatory elements of the Privacy Notice:

(4) identity and contact details of the controller;

(5) contact details of the data protection officer;

(6) purposes of processing for which personal data are used as well as the legal basis for processing and recipients or categories of recipients of personal data (if any);

(7) additional information covering the period in which the personal data to be stored or, if not possible, the criteria which determine this period;

(8) information on the rights of users and the method of fulfilling these rights, the existence of the rights of users and how to achieve them;

(9) information on whether the provision of personal data is necessary and what are the consequences if the user does not provide them; and

(10) information on the use of data for automatic profiling of the user (by what logic does the profiling and what are the consequences for the user).

Research limitations

In general, research on organizational practices related to privacy shows the extent to which organizations provide privacy, which include privacy policies and whether they are in line with standards and/or expectations of users, but do not provide answers as to why and why something affects privacy.

Findings and discussion

The study covered all national libraries in Europe, a total of 45. National libraries of EU member states: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Croatia, Ireland, Italy - Rome, Italy - Florence, Latvia, Lithuania,

Luxembourg, Hungary, Malta, The Netherlands, Germany, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the national libraries of non-EU countries: Albania, Belarus, Bosnia and Herzegovina, Montenegro, Iceland, Kosovo, Liechtenstein, Macedonia, Moldova, Serbia, Switzerland, Norway, UK (England, Scotland, Wales, Northern Ireland) and Ukraine.

Of the 28 national libraries of the Member States of the European Union, 10 do not have a separate web page site with a privacy notice that relates to the content of users' general personal data (Belgium, Bulgaria, Cyprus, Czech Republic, France, Greece, Latvia, Lithuania, Romania and Slovenia) (Figure 1). Of the ten not having a page dedicated to information regarding the protection of personal data, seven of them still have a prominent privacy notice related to cookies or the use of library websites, and three do not have a statement about cookies.

Of the 28 national libraries of the EU Member States, 15 have both the page dedicated to personal data protection and a separate cookie statement. Three of them have only separate pages dedicated to personal data protection and seven have only separate cookie statements. Three of the libraries researched have not published a privacy notice as a part of their website nor have made available any kind of notice or statement regarding the use of cookies.

Of the 17 libraries in non-EU countries, most (nine) have published at least partial information dedicated to personal data protection (Iceland, Liechtenstein, Moldova, Northern Ireland, Scotland, Switzerland, Norway, England and Wales) (Figure 2). Most libraries (ten of them) do not have a cookie statement that would be visible as soon as the website is accessed.

Two of the libraries only have a page with a privacy notice and eight of the libraries in question have published no privacy related information.

According to the criteria of the transparency guidelines on the publication of privacy notices, it was found that out of a total of 18 national libraries of EU Member States that have a special website dedicated to privacy, 15 of them publish a privacy notice in a layered form. As mentioned earlier, other libraries in the European Union state the rules for the protection of users' personal data in their notices on the use of services, but do not meet the criteria of a "layered" privacy notice and do not belong to this group for analysis.

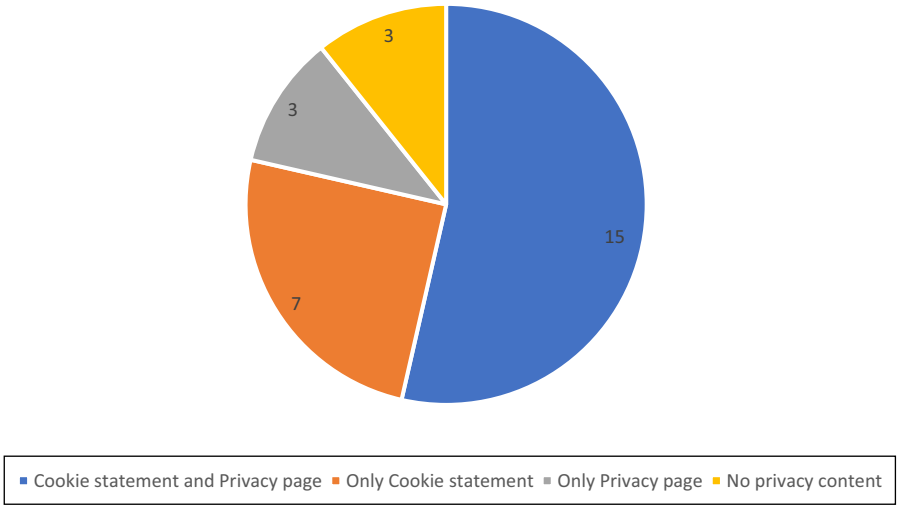

Figure 1.
Presence of separate privacy pages/notices of national libraries of the EU Member States

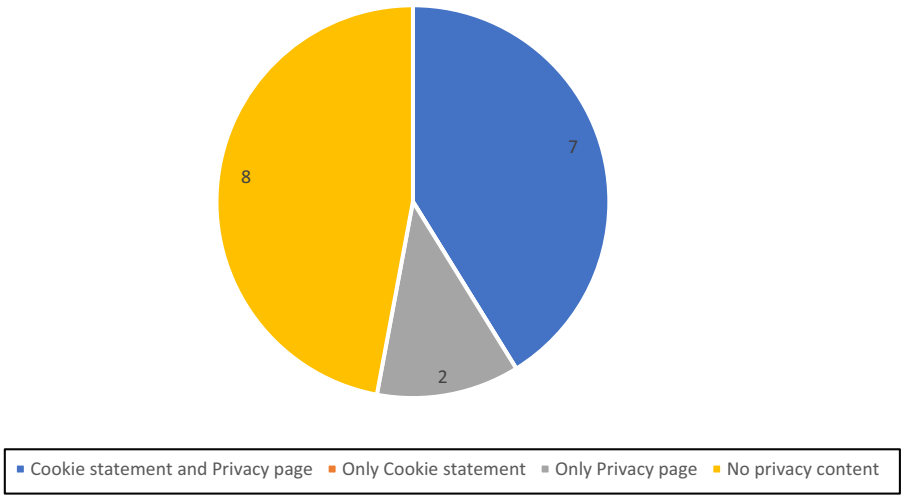

Figure 2.
Identification of separate privacy pages/notices of national libraries of non-EU Member States

There are two forms of layered notice visible in practice: some libraries have a layered notice in the sense that at the beginning of the document all subheadings or units related to specific types of information are highlighted, so clicking on a particular subheading opens the content for more information. Other libraries have layered notices in the sense that the text contains additional links for more information on certain topics (individual privacy notices for certain purposes or links to the rules on the use of library services and materials). Both forms are appropriate for the library user and do not contain excessive information and in that sense represent a "layered" notice.

The next criterion for analysis is the criterion of mandatory elements according to Art. 13 of GDPR. 17 national libraries of the Member States have properly referenced themselves and provided contacts as data controllers (Figure 3). Seven of them provided information on collecting data when using the library's website and web services, but not on the conditions for processing personal data when joining or providing other services to the user. As Art. 13(4) of GDPR states that this information does not need to be provided if the data subject already has the information, privacy notices for personal data processed by libraries may have been provided in another way. For example, a notice to users may have been provided in hard copy at the time of user enrollment.

The most common shortcoming of the mandatory element is information on what personal data is necessary and what the consequences are if the data subject does not provide it.

Interestingly, of the nine national libraries of non-EU countries that have Web pages dedicated to privacy, eight have a very detailed privacy notice adhering to the Transparency Guidelines (Figure 4).

The best examples are the National Libraries of England, Scotland and Norway as they have published privacy notices for each purpose of processing personal data. Thus, privacy notices are presented in layered form with a general privacy policy and definitions for the following purposes: procurement and rental of materials, surveillance camera videos, collections, communication, tenders, contact information, online donations, employment, inquiries, reservation of seats on event, feedback and complaints, fundraising, compliance, purchase, member registration, security, *wifi*, privacy statements for commercial services, account creation, education and learning purposes, marketing, social networks, use of online library, subscription to newsletter, video streaming during a library event.

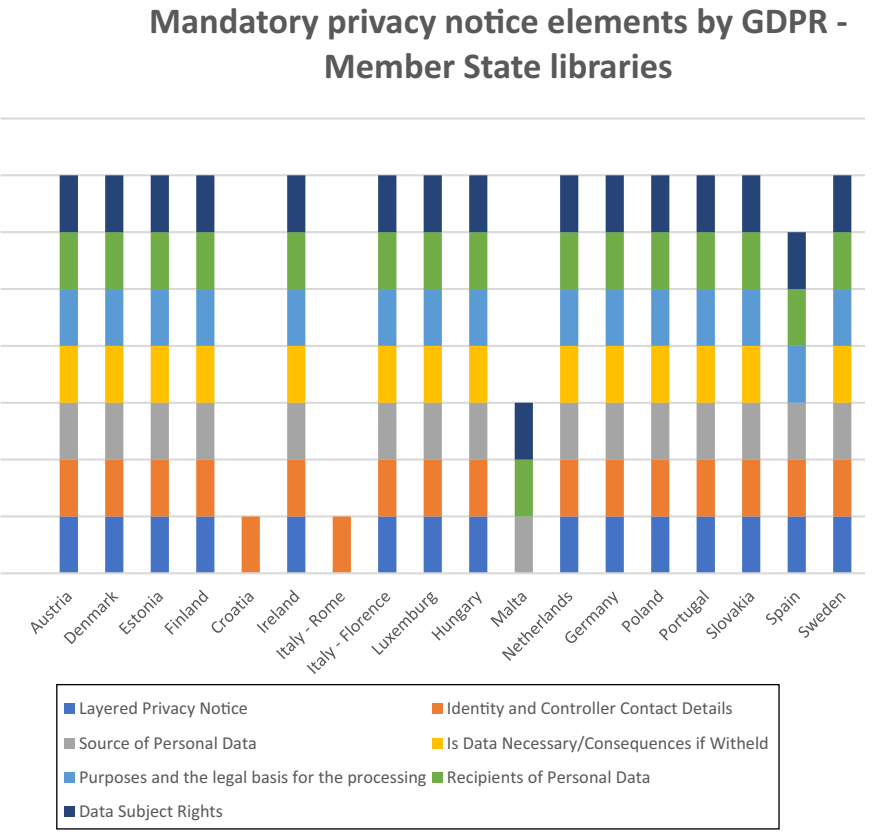

Figure 3.
National libraries of EU Member States that have a separate privacy page/notice

Scope for further studies

Since the GDPR was adopted in 2016 and has been in full implementation since May 2018, scarce research relevant and related to librarianship has been published in Europe, especially regarding the application of the data protection principles. In general, finding out the effectiveness of measures libraries apply as data controllers to ensure safe and secure processing of patron personal data presents an interesting research topic.

Recommendation for the further research would be to examine the expectations and satisfaction of library users with fulfilling their rights to personal data protection in libraries as well as research on the role of regional/state library societies in supporting libraries to comply with GDPR or understanding the new legal framework.

Conclusion

GDPR has had a profound impact on the state of library data protection compliance. As data controllers, libraries are obliged to implement adequate mechanisms and procedures that greatly enhance transparency and inform patrons on the contents of their rights. As the general level of data protection awareness rises, the library patrons (aka data subjects) will be empowered to exercise their rights and create additional impetus for libraries to develop

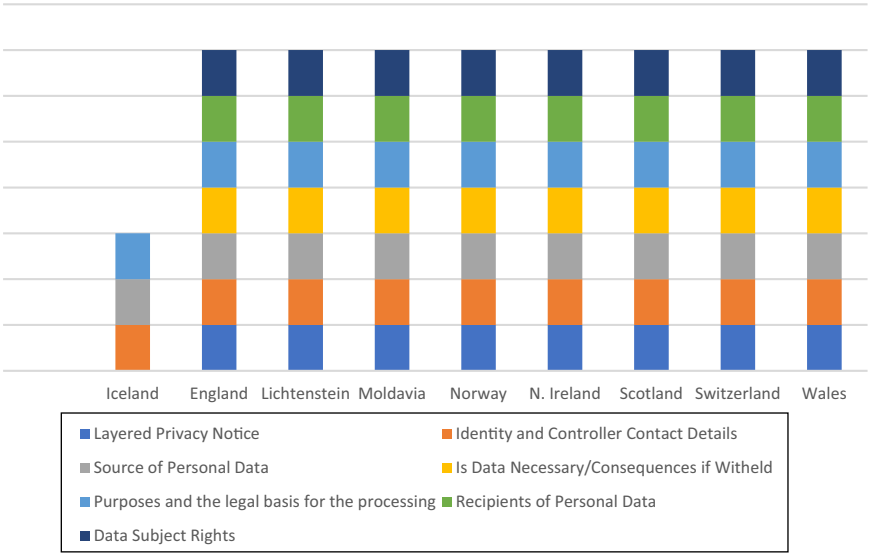

Figure 4.
National libraries of non-EU countries that have a separate privacy page/notice

in this regard. Research has helped show that the legal framework of data protection has positively contributed to the level of transparency of personal data processing in libraries.

The authors generally expected that the new legal framework and accompanying guidelines clarifying the implementation of the principles of personal data processing represented an opportunity to raise the quality of personal data protection both for organizations in the EU Member States as well as those based in countries not required to adhere to the GDPR, as these obligations promote transparent processing of personal data, and that this opportunity was at least partially taken by library organizations to improve their practices.

The first research question of how and in what manner do European national libraries use privacy notices to communicate with users about the processing of personal data yields an answer that 27 out of 45 (60%) libraries use a privacy notice, and 29 a cookie notice (64%), generally supporting the notion that most libraries adequately observe the principle of transparency. Eleven libraries (24%) of surveyed websites published no privacy notices or cookie notices.

With regard to following established transparency guidelines, the survey showed that 51% of European national libraries have implemented privacy notices adequately in line with the WP29/EDPB Transparency Guidelines and have enabled their users with access to all the necessary information on the processing of personal data in an accessible and clear way. There are 64% of libraries of EU-member State that have a separate privacy page in contrast to 52% of the non-member State libraries.

According to the obtained data, it is evident that libraries belonging to EU Member States to a greater extent respect the principle of transparency, and it can be concluded that the application of GDPR has contributed to the transparency of personal data processing in national libraries in Europe.

It is interesting that libraries of non-EU countries, which have actually undertaken data protection compliance efforts, approached the implementation of the principle of transparency with quality and adequate understanding of fundamental data protection principles as reflected in the findings. At the time of our research, 53% of the EU Member State national libraries websites managed to comply with publishing all necessary data

protection information in a way recommended by the Guidelines, compared to 47% of non-Member State national libraries.

Another issue explored was to establish to what extent do libraries state the purposes and legal bases for all processing of personal data in the notices. Out of 27 libraries that have separate privacy page, 24 include a privacy notice with adequate information on purposes and legal bases for their personal data processing activities, implying that informed and responsible compliance efforts were undertaken.

The relationship between the library and the user is based on confidentiality. One way to help show that the library adequately protects the user's interests is to publish privacy notices on its website. According to the data obtained, it can be concluded that many libraries do not implement all applicable measures to foster a relationship of trust with the user, and that there is room for improvement in the communication of personal data processing to the user. Like many public institutions, libraries need additional guidance, perhaps even dedicated sectoral guidance by the supervisory bodies to foster a more transparent and effective personal data protection efforts and better communication of these efforts to their patrons.

Note

1. Cookies (eng. Cookies) are small data files that websites leave on users' computers via the Web browser to monitor the operation and habits of users. Under European Union law, we distinguish between cookies that are necessary for the proper operation of the website and those that are not necessary. To use these others, Union law requires the consent of the user of the website.

References

Bailey, J. (2018), "Data protection in UK library and information services: are we ready for GDPR?", *Legal Information Management*, Vol. 18 No. 1, pp. 28-34, doi: 10.1017/S1472669618000063.

Caldwell-Stone, D., (2015), "The law regarding privacy and confidentiality in libraries", in Magi, T., M. and Garnar, (Eds.), *Intellectual Freedom Manual: 10th Edition*, American Library Association, pp. 184-200.

Charillon, A., Peachey, J. and Heydecker, R. (2018), *Leading the Way – a Guide to Privacy for Public Library Staff*, Carnegie UK Trust, City Library, CILIP, Dunfermline, London, Newcastle upon Tyne, available at: www.carnegieuktrust.org.uk/publications/leading-the-way-a-guide-to-privacy-for-public-library-staff/

Gonzalez Fuster, G. (2014), *Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer

Gorman, M. (2015), *Our Enduring Values Revisited: Librarianship in an Ever-Changing World*, ALA Editions, Chicago.

IFLA Statement on Libraries and Development (2013), available at: www.ifla.org/wp-content/uploads/2019/05/assets/alp/statement_on_libraries_and_development.pdf

IFLA Statement on Privacy in the Library Environment (2015), available at: www.ifla.org/wp-content/uploads/2019/05/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf

Iglezakis, I., *et al.* (2011), "Personal data protection in digital libraries", in Iglezakis, I. (Ed.), *E-Publishing and Digital Libraries: Legal and Organizational Issues*, IGI Global, pp. 413-429, doi: 10.4018/978-1-60960-031-0.ch019.

Koops, B.J., Newell, B.C., Timan, T., Skorvanek, I., Chokrevski, T. and Galič, M. (2016), "A typology of privacy", *University of Pennsylvania Journal of International Law*, Vol. 38, pp. 483-575.

Lambert, P. (2018), *Understanding the New European Data Protection Rules*, Taylor and Francis

Noh, Y. (2017), "A critical literature analysis of library and user privacy", *International Journal of Knowledge Content Development and Technology*, Vol. 7 No. 2, pp. 53-83.

Pedley, P. (2020), *A Practical Guide to Privacy in Libraries*, Facet Publishing, London.

Richards, N.M. (2008), "Intellectual privacy", *Texas Law Review*, Vol. 87, pp. 387-445, available at: https://ssrn.com/abstract=1108268

Richards, N.M. (2015), *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Oxford University Press, Oxford.

Schepmann, T., Koren, M., Horvat, A., Kurtović, D. and Hebrang Grgić, I. (2008), "Anonimity of library users in The Netherlands and Croatia", *New Library World*, Vol. 109 Nos 9/10, pp. 407-418, doi: 10.1108/03074800810910441.

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C. and Hardy, R. (2003), "User privacy in the digital library environment: an investigation of policies and preparedness", *Library Management*, Vol. 24 Nos 1/2, pp. 44-50.

Voigt, P. and von Dem Bussche, A. (2017), *The EU General Data Protection Regulation (GDPR): a Practical Guide*, Springer

Zimmer, M. (2013), "Assessing the treatment of patron privacy in library 2.0 literature", *Information Technology and Libraries*, Vol. 32 No. 2, pp. 29-41, doi: 10.6017/ital.v32i2.3420.

Further reading

Article 29 Working Party Guidelines on Transparency under Regulation (2018), 2016/679, available at: https://ec.europa.eu/newsroom/article29/items/622227/en

Charter of Fundamental Rights of the European Union (2012), "/C 326/02", available at: https://eur-lex.europa.eu/eli/treaty/char_2012/oj

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", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

Guidelines 3/2018 (2019), "On the territorial scope of the GDPR (article 3) - version adopted after public consultation", available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf

Handbook on European Data Protection Law (2018), "Publications office of the European Union, Luxembourg", available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

IFLA Code of Ethics for Librarians and other Information Workers (2012), available at: www.ifla.org/wp-content/uploads/2019/05/assets/faife/publications/IFLA%20Code%20of%20Ethics%20-%20Long_0.pdf

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)", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Strasbourg (1981), "Convention for the protection of individuals with regard to automatic processing of personal data", Treaty No. 108., 28th January 1981, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

Corresponding author
Anita Katulić can be contacted at: akatulic@nsk.hr