Issue Brief

The General Data Protection Regulation: What Does It Mean for Libraries Worldwide?

May 2018

ASSOCIATION OF RESEARCH LIBRARIES

Introduction

Krista L. Cox, Director of Public Policy Initiatives, Association of Research Libraries

The General Data Protection Regulation (GDPR), a binding European Union (EU) law governing data protection and privacy for citizens and residents of the EU and the European Economic Area, will go into force on May 25, 2018. GDPR, a robust privacy framework, aims to give more control to individuals over their personal data. Businesses and others collecting data must ensure that full disclosures are made and consent is freely given by the individuals whose data is being collected.

GDPR grants individuals six specific rights with respect to their data including: (1) information and access (i.e., to know that their personal data is being processed and have access to this data free of charge); (2) data portability (data collected under certain circumstances must be provided "in a structured, commonly used, and machine-readable form"; (3) rectification (ability to correct inaccurate personal data or to complete information); (4) erasure (also known as the "right to be forgotten," applicable only under certain circumstances); (5) restriction (individual may restrict data controller from processing data further under certain circumstances); and (6) objection (to object to processing of one's data).

Although GDPR is an EU regulation, it has implications for businesses and institutions that collect data even outside the EU. Anne T. Gilliland, scholarly communications officer at the University of North Carolina at Chapel Hill Libraries, explains some of the key provisions of GDPR and why its impact reaches worldwide. Gilliland notes that the research library community has ties to Europe and EU citizens. Libraries must therefore consider the implications GDPR will have on their own privacy policies and how to ensure compliance with these new rules. As staunch defenders of privacy rights, libraries have an opportunity to ensure robust protection of users' rights. Because GDPR has not

yet gone into effect, there is no case law or other binding guidance regarding GDPR compliance.

The Association of Research Libraries will continue to monitor developments on GDPR and will publish a follow-up piece focusing on implementation. In the meantime, the following resources may be useful:

- EU's GDPR Information Portal
- Library of Congress, "Online Privacy Law: European Union"
- LIBER, Webinar Video: "GDPR & What It Means for Researchers"

The General Data Protection Regulation: What Does It Mean for Libraries Worldwide?

Anne T. Gilliland, Scholarly Communications Officer, University Libraries, University of North Carolina at Chapel Hill

In the last few months you may have received emails from companies or seen notices on websites saying such things as, "The way we communicate with you is changing," or "You must opt in to keep getting emails from us." These are examples of responses to the European Union's (EU's) General Data Protection Regulation (GDPR), which will take effect May 25, 2018. The GDPR, which Daniel Solove, a law professor and privacy expert at The George Washington University, has called "the most profound privacy law of our generation,"[1] is likely to have a significant impact on the way all of us deal with and manage personal data.

Scope of the GDPR

The GDPR's scope is broad in almost every way, and it aims to cover the handling of personal data as it occurs in the full range of commercial and professional activities as they pertain to EU citizens and residents. The GDPR applies even when EU citizens are living or visiting outside of Europe. The law's goals include full accountability, consistency, and transparency from the organizations that collect and use personal data, and complete understanding and meaningful consent from the subjects whose data is being used.[2] In contrast, in the United States, we have a patchwork of federal and state privacy laws and regulations that are limited by jurisdiction, by type of data or class of person, by the type of activity using the data, and by the technology used. We have not, to date, experienced laws mandating the consistency and transparency in the handling of personal data that the GDPR requires.

At the same time, the GDPR is forcing significant, difficult changes in

the ways that companies and organizations do business **worldwide**. It is difficult, if not impossible for companies to handle EU personal data differently from the personal data of the rest of the world, and so companies must apply GDPR requirements uniformly to all the personal data they collect or handle. Because of their various ties to Europe and EU citizens, such as exchange programs, study abroad opportunities, visiting scholars, and satellite campuses in other countries, universities and research libraries are among the organizations that now must come to terms with the GDPR's requirements. For some FAQs from the European Union on their rationale for enacting the GDPR and the benefits from it that they envision, see "Questions and Answers—General Data Protection Regulation."[3] The EU has also issued a fact sheet, "The GDPR: New Opportunities, New Obligations,"[4] which briefly highlights the GDPR's key provisions.

Some of the GDPR's Provisions

The GDPR covers the entire spectrum of the ways that personal data is managed and transferred, and it forces organizations to take stock of what data they collect, how they collect it, and how they manage it. The law requires that companies provide comprehensive data privacy training for staff and makes organizations liable with significant penalties if there are data breaches or lapses. One big privacy concern today is personally identifiable information, data that does not positively identify an individual but that allows a person's identity to be deduced. For example, one of the most famous examples of re-identification from disparate pieces of data occurred in 1997 when a researcher identified the medical history of William Weld, the governor of Massachusetts, from anonymized health data. The researcher did this by combining open health data that had been anonymized but still included information on each patient's age, sex, and ZIP code, with public information from the voter registration rolls.[5] In an effort to prevent these sorts of scenarios, the GDPR regulates both identified

and identifiable data. It also regulates situations where organizations transfer data and subcontract data management, holding both data controllers and data processors accountable.

The GDPR is configured to defend an individual's rights robustly. Many privacy laws in the US, such as the Health Insurance Portability and Accountability Act (HIPAA), have no private cause of action. An individual who is the subject of a data breach cannot use HIPAA to sue and recover damages. Similarly, the US Supreme Court has held that the Family Educational Rights and Privacy Act (FERPA), which safeguards students' privacy in the United States, does not allow a private cause of action.[6] Under the GDPR, however, European citizens and residents will be able to sue for privacy breaches and will be able to collect damages even when they have suffered reputational harm, breach of trust, or increased risk, but no immediate monetary harm. Individuals may also receive other redress, such as the right to be forgotten or the right to have errors in their data corrected. The GDPR requires an individual's explicit consent, or "opt in," when an organization collects personal information; it is not enough to obtain consent through an opt-out policy or an individual's inaction. This is also in contrast with FERPA, which starts with the assumption that directory information is public and then allows students to opt out.[7]

Conclusion

Although there are still many questions about how the GDPR will work and interact with the laws of other countries, it seems clear that the EU's new law will change the way that large organizations all over the world—including libraries—collect and handle personal data. These changes are likely to be painful and expensive, but they also hold the promise of providing far more meaningful ways to control and safeguard personal data. In the wake of such incidents as the Cambridge Analytica revelations, libraries, as privacy champions, should welcome the GDPR's requirements.

Endnotes

1. Daniel Solove, "Why I Love the GDPR: 10 Reasons," *TeachPrivacy Privacy + Security Blog*, May 2, 2018, https://teachprivacy.com/why-i-love-the-gdpr/.

2. For the full text of the GDPR in English, see "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)," *Official Journal of the European Union: Legislation*, 59 (May 4, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

3. European Commission, "Questions and Answers—General Data Protection Regulation," January 24, 2018, http://europa.eu/rapid/press-release_MEMO-18-387_en.htm.

4. European Commission, *The GDPR: New Opportunities, New Obligations* (Luxembourg: Publications Office of the European Union, 2018), https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf.

5. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, 57 (2010): 1701, 1719–22, https://www.uclalawreview.org/pdf/57-6-3.pdf.

6. Gonzaga v. Doe, 536 US 273 (2002).

7. Barmak Nassirian, "The General Data Protection Regulation Explained," *EDUCAUSE Review*, August 28, 2017, https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained.

ASSOCIATION OF RESEARCH LIBRARIES

Association of Research Libraries
21 Dupont Circle, NW
Suite 800
Washington, DC 20036
T 202.296.2296
F 202.872.0884

ARL.org
pubs@arl.org