GOVERNMENT AND REGULATORY AFFAIRS BLAST

Preparing for GDPR – There's Still Time!

March 2018

By Cathie T. Chancellor, JD, MS, CRM

STATUTE/REGULATION SOURCE

Regulation (EU) 2016/679 of the European Parliament and of the Council, April 27, 2016

BRIEF DESCRIPTION

The General Data Protection Regulation (GDPR) was adopted in 2016 and becomes effective May 25, 2018. The GDPR promotes uniformity and expands personal privacy rights for European Union (EU) residents. The regulation replaces the 1995 Data Protection Directive (DPD) and increases relative enforceability. It impacts entities, such as higher education institutions, which control or process covered personal information, even if such institutions have no physical EU presence. This means US institutions with EU-based operations and/or with significant numbers of EU residents who are students — including students within the EU receiving distance education programs — must comply with GDPR!

POTENTIAL/ACTUAL IMPACT

According to the EU, personal data is any information related to a natural person (called a "data subject") that can be used directly or indirectly to identify the person. It can be a name, a photo, an email address, bank details, social networking posts, medical information or a computer IP address.

The GDPR will apply to information collected about people who have permanent residence in the EU and countries falling within the EEA (European Economic Area). It's important, though, to make the distinction that "only information of natural persons is in scope, and corporate data is out of scope".[1] The GDPR will not apply to EU nationals having permanent residence outside of the EU.

Institutions that control or process personal data as a part of their business or on behalf of another entity will have to comply with the GDPR. The GDPR will apply not only to organizations located within the EU, but it will also apply to organizations located outside of the EU, if those organizations offer goods or services to, or monitor, the behavior of EU data subjects. In short, it will apply to all business entities processing and holding the personal data of individuals residing in the EU, regardless of the entity's location.

The maximum fine for breaching the GDPR that will be imposed on an organization for the most serious type of infringement is four percent of annual global turnover or €20 million. There will be a tiered approach to fines. For example, a business could be fined just two percent of annual global turnover for not having their records in order (*Article 28*), not notifying the supervising authority about a breach, not notifying a data subject about a breach or not conducting impact assessment(s). It's important to note that these rules apply to controllers and processors of information, and that cloud applications and software are not exempt from GDPR enforcement.[2]

1. Christopher Rau, Jens Krickhahn and Marek Stanislawski, "GDPR – Highlights You Need to Know," Allianz, February 20, 2018, 1 (http://www.agcs.allianz.com/insights/expert-risk-articles/grd-gdpr/)
2. "GDPR FAQs," EU GDPR (https://www.eugdpr.org/gdpr-faqs.html)

Preparing for GDPR – There's Still Time!

March 2018

DISCUSSION

The US and the EU have different approaches to privacy law. Adhering to a sectoral approach, the US privacy laws are formed when needed, and sector industries become well-acquainted primarily with their sector's areas of compliance and related issues. In contrast, the 28 member states of the EU view privacy as a fundamental human right and take a more comprehensive approach to privacy law. In May 2018, they will implement the GDPR as a single law to govern the collection of all information and data about EU citizens.

The GDPR requires that no personal data collection or usage should occur without the notice and consent of the individual. It specifies more comprehensive requirements for notice and consent than most US privacy laws. For notification to be clear and transparent, the notice will have to 1) be concise, intelligible and easily acceptable; 2) use clear and plain language; 3) be in writing or other accepted means; and 4) be provided free of charge. In addition to transparency criteria, the GDPR outlines specific transparency content requirements, including 1) the identity and contact information of the entity collecting the data; 2) the purpose and legal basis for processing and/or use of data; 3) the recipients of the information; 4) details of any transfers of information to another country outside of the EU; 5) the retention period; 6) the individual's rights to the data used; 7) the process of consent withdrawal; 8) whether data is profiled or auto-processed; and 9) what information, if any, is required to be provided, and what happens if information is not provided.[3]

GDPR requirements essentially include, but are not limited to:

- Implementing certain policies and processes
- Developing an effective internal data protections management system
- In many instances, appointing a data protection officer

ACTION

The implication of the GDPR is that US industries and institutions will have to develop new compliance mechanisms, procedures and policies to mitigate these additional risks and challenges! Here are some steps you can take.

- Learn about the GDPR directly at https://www.eugdpr.org/
- Read "The General Data Protection Regulation: A Primer for U.S.-Based Organizations That Handle EU Personal Data" by Caroline Krass, Jason N. Kleinwaks, Ahmed Baladi, and Emmanuelle Bartoli on *Compliance & Enforcement*, New York University School of Law's Program on Corporate Compliance and Enforcement.
- Make sure you and others connected to your institution fully understand and document when and where personal data is being collected, how it is being used and how the institution is protecting it.
- Review your institution's policies and procedures for sharing information, and identify potential exposures.

3. Cara M. Johnson, "What's in a notice? Privacy notice under the GDPR," *Privacy & Data Security Insight*, February 28, 2018 (https://www.privacyanddatasecurityinsight.com/2018/02/whats-in-a-notice-privacy-notices-under-the-gdpr/#page=1)

Preparing for GDPR – There's Still Time!
March 2018

- Attend the Global Privacy Summit, March 27-28, 2018, in Washington, DC, with certification training March 25-26. https://iapp.org/conference/global-privacy-summit-2018/
  Otherwise, consider contacting the International Association of Privacy Professionals (IAPP) concerning the availability of post-Summit presentations or notes. https://iapp.org/about/contact/

- Make sure risk management staff have minimum-to-high-level involvement with GDPR projects at your institution. Although everyone at your institution very likely knows that maintaining cyber security and preventing exposures are key risks, everyone also needs to understand that maintaining data privacy is an ongoing key risk as well. As insurer Allianz advises, "The GDPR also requires 'privacy by design' and 'privacy by default' to encourage data protection from the earliest stage of any project or initiative. A robust privacy check early in the beginning of every project or new process will become a mandatory internal requirement. Since the GDPR is not a one-off implementation, it will require a continuous risk approach."[4]

- Collaborate with ALL stakeholder departments responsible for travel abroad, distance learning programs, research and more to ensure not only the safety and security of travelers, but also their personal data.

- Understand your cyber insurance. Talk with your agent or broker about liability coverage and breach response service options. Understand what your provider can do to augment your current policies and procedures. If a GDPR compliance violation occurs, it will be beneficial to demonstrate that your institution has taken added steps to protect personal data.

SOURCES AND REFERENCES

- EU GDPR: https://www.eugdpr.org/

- GDPR: Report: https://gdpr.report/

- Caroline Krass, Jason N. Kleinwaks, Ahmed Baladi, and Emmanuelle Bartoli, "The General Data Protection Regulation: A Primer for U.S.-Based Organizations That Handle EU Personal Data," *Compliance & Enforcement*, New York University School of Law's Program on Corporate Compliance and Enforcement, December 11, 2017: https://wp.nyu.edu/compliance_enforcement/2017/12/11/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/

- Ann Kristin Glenster and Katelyn Ilkani, "Cybersecurity Series: GDPR and Higher Education Institutions," The Tambellini Group, August 2017: https://www.thetambellinigroup.com/post/cybersecurity-series-gdpr-and-higher-education-institutions/

- EDUCAUSE Library: EU General Data Protection Regulation (GDPR): https://library.educause.edu/topics/policy-and-law/eu-general-data-protection-regulation-gdpr

4. Rau, 2

Preparing for GDPR – There's Still Time!

March 2018

- 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
- *Privacy & Data Security Insight* GDPR Archives: https://www.privacyanddatasecurityinsight.com/tag/gdpr/
- EUR-Lex: Access to European Union Law: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- Brain Eaton, "GDPR: How is it Different from U.S. Law & Why this Matters?" *Privacy & Data Security Insight*, September 14, 2017: https://www.privacyanddatasecurityinsight.com/2017/09/gdpr-how-is-it-different-from-u-s-law-why-this-matters/#page=1

URMIA's Government and Regulatory Affairs Committee (GRAC) serves as a resource for informing and educating URMIA's members about federal legislation and regulations. Todd Beekley, University of Cincinnati, currently serves as its chair. If you would like to be a member or have a topic for a future Regulatory Blast, contact the URMIA National Office (urmia@urmia.