THE GENERAL DATA PROTECTION REGULATION IS HERE, AND IT’S NOT GOING ANYWHERE

BY SHANE DEMPSEY
In May 2018, the European Union’s General Data Protection Regulation (GDPR) went into effect. While the main impetus for this wide-reaching regulatory action was to give citizens in the EU greater control over how organizations process their personal information, the implications are worldwide and touch upon many industries—and libraries are not exempt. The GDPR requires companies that process personal information to follow the GDPR tenets or face painful monetary sanctions (up to 4% of global revenue or €20 million, whichever is greatest!).

The territorial scope of the GDPR raises very complicated issues for individuals, companies, organizations, and governments—the true meaning of which is still being sorted through as we find ourselves in a brave new privacy-concerned world. For example, the GDPR applies even when non-EU based companies offer services to individuals living in the EU, whether they are EU citizens or not.

**How and Why Did We Get Here?**

Since the dawn of the internet, people have been giving away their personal information in return for a slew of free services such as email, social networks, entertainment, online shopping, and travel assistance. Concerns about privacy barely registered with the public, even though the Wild West reputation of the early internet should have raised warning flags.

Almost everything we do in our modern lives can be broken down into bits of data, much of which could be used to piece together the personally identifiable information of individuals. Yet, barely a month goes by without news of another data breach in some industry and the subsequent exposure of personal data that could be used to identify individuals and expose them to fraud, theft, or other criminality.

So, it makes perfect sense that any coherent idea of a globalized digital marketplace must be based on trust. And the only way to accomplish that is with a broad set of common standards for data processing and protection that simplifies the regulatory environment so that both citizens and businesses can benefit. And that is where the GDPR comes in.

**How Is the GDPR Relevant for Libraries?**

Libraries—whether they are located in the city center, a university campus, a law firm, a court house, or a building on Main Street—have been on the forefront of the digitization of records that contain all types of personal information; therefore, every library that has any interactions or transactions with users in the EU needs to comply with the GDPR. It is highly impractical, and potentially dangerous, to handle data differently between EU and non-EU individuals.
Libraries almost always require at least a name, a street address, and an email address before a user can access materials. Some libraries collect credit card information, an especially tempting target for criminal hackers. Libraries also track the borrowing history of users, and that history could tell others more about a person than they would normally give consent to be shared. Imagine how much drug companies would pay to obtain information on which individuals checked out books on diseases such as cancer or diabetes.

And even though libraries are not normally in the business of selling aggregated data about their users or tracking behavioral patterns that lead to direct marketing from any of this information, they must be highly vigilant when it comes to their internal procedures and how they interact with individuals.

Libraries may benefit from the fact that one of the key aspects of the GDPR, the so-called “Privacy by Design” concept (i.e., implementing GDPR principles into processing activities, from the coding done in the design stage all the way through the entire data lifecycle), has been part of our operational and technological model for a long time.

What Are the Main Consequences of GDPR for Libraries?

Legal Basis

Libraries of all types must have a legal basis for processing personal data of EU citizens. Libraries may rely on one of the following grounds:

- The positive consent of the user, also known as “Opt-in”
- Processing is necessary for the performance of a contract with the user
- Processing is required for compliance with legal obligations
- Processing is in the public interest
- Processing is in the library’s legitimate interest and is not overridden by the user’s rights and interests

Exemptions for Libraries

There are some specific, limited, exemptions in the GDPR that relate to how libraries operate. There are archival exemptions for those libraries that archive materials in the public interest—there is a legal obligation to perform these activities, so these exemptions would mostly pertain to public or university libraries. There are other exemptions for historical or scientific research, and this includes statistical analysis of personal data. These exemptions are not mandatory for all EU Member States and may be implemented by them, so careful adherence and knowledge of applicable country laws would be necessary.

A more powerful exemption is the one based on freedom of expression. As it is acknowledged that libraries play a crucial role in preserving the freedom of expression through the holding of news, press, and TV broadcast material, they may gain exemptions that reduce the burdens of the regulation.

Security and Breach Notification

Libraries also have new, extremely important responsibilities that must be strictly adhered to, such as ensuring the security of the personal information we hold and notifying authorities within 72 hours if there has been a data breach of any kind. In some cases, where there is a high risk for the individual’s rights and freedoms, the users affected must also be notified as soon as possible. Failure to do either will lead to severe financial penalties.

Data Transfer Outside of the EU

Another key issue concerns the restrictions on transferring personal data outside the EU. Libraries can only transfer personal data to countries that offer an adequate level of protection of personal data according to the EU, or if they have implemented appropriate GDPR
These rights include:

Privacy Policy
We must also ensure that any contractual terms and conditions are expressed in understandable, layman’s terms, along with clear explanations for the usage of an individual’s personal data. Adopting a privacy policy is generally seen as a good way to comply with these requirements.

Individuals’ Rights
Perhaps most importantly, there is now a new digital bill of rights for every individual that all libraries need to understand and know how to comply with and integrate into their privacy policies. These rights include:

- The right to be informed about the collection and use of personal data—this requires libraries to draft privacy policies and notices to inform users.
- The right of access to personal data, including a copy of the data being processed.
- The right to rectify any inaccurate or incomplete personal data.
- The right of erasure of personal data if it is no longer needed for the original purpose it was collected, or if consent is withdrawn, or if the data has been processed unlawfully, or if the erasure is necessary for compliance with EU law. This is also known as the “right to be forgotten.”
- The right to restrict processing of personal data if the accuracy is contested, the processing unlawful, the user objected to the processing, or the information is no longer needed for the purposes of processing.
- The right to data portability allows individuals to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- The right to object to processing must be obeyed unless the processor can demonstrate that there are legitimate grounds for overriding the objection.
- The right to not be subject to automated processing such as profiling, which produces legal effects concerning the individual or similarly significantly affects him or her, unless it is necessary for the entering or performance of a contract, or it is allowed by EU or Member State law, or the individual themselves.

Data Processing Agreements
Libraries must also ensure the companies that process personal data on their behalf (such as cloud service providers) comply with the GDPR. Libraries are required to have appropriate processing agreements in place with such companies.

The Libraries’ Role in the GDPR Environment
Libraries will play an important role in this new GDPR environment, as we are well placed to assist our users by helping them navigate the new controls over how their data is collected, processed, and transferred.

Libraries will play an important role in this new GDPR environment, as we are well placed to assist our users by helping them navigate the new controls over how their data is collected, processed, and transferred.

- The right to object to processing must be obeyed unless the processor can demonstrate that there are legitimate grounds for overriding the objection.
- The right to not be subject to automated processing such as profiling, which produces legal effects concerning the individual or similarly significantly affects him or her, unless it is necessary for the entering or performance of a contract, or it is allowed by EU or Member State law, or the individual themselves.

Information Management

SHANE DEMPSEY
SENIOR RESEARCH AND REFERENCE SPECIALIST
WilmerHale
Brussels, Belgium
Shane.Dempsey@wilmerhale.com

Shane Dempsey is a senior research and reference specialist in the WilmerHale Brussels office. In his role, Dempsey is responsible for assisting the global library team in responding to complicated research projects sent from all WilmerHale offices, worldwide. He also works closely with Brussels-based client matter teams on large antitrust and merger notification cases. He has been assisting lawyers as they work through the implications of the GDPR for the firm and its clients. Leveraging this network, his main focus has been on tearing down geographical silos and building out the idea of a global research team. He often presents seminars to the entire library staff on this issue with the goal of increasing efficiency, awareness, and internal client satisfaction.