International Federation of Library Associations and Institutions

Briefing: Impact of the General Data Protection Regulation 2018[1]

The EU General Data Protection Regulation comes into force across the European Union on May 25th 2018. It is very important for libraries and archives to start work now to comply with the new regulation, which puts a positive obligation on organisations to responsibly protect and use information that identifies a living person. This type of personal information is referred to as "personal data" and can include names, addresses, email addresses, IP addresses, library card numbers, phone numbers etc.

This briefing is not comprehensive, but is intended as a way to help libraries think about what they need to do in order to be prepared for the new law.

What are the main changes for organisations?

- **Higher Penalties.** Higher penalties of up to €20 million or 4% of global turnover, are possible for more serious infringements of core principles of the regulation. For example if relying on consent from an individual to use their personal information when registering at the library, the terms and conditions must clearly and in plain language explain how their information is being used. [2]
- **Privacy by Design.** This legal term means that organisations must proactively "design in" technical and organisational processes that comply with data protection law. For example you should not hold more personal information than is actually required or keep personal data for longer than is needed. You must ensure your IT systems are safe also, and encryption or pseudonymisation[3] is strongly encouraged. It is also important that when you plan new processes or IT systems, that you do an assessment on how the personal information being held by the library will be affected[4].
- **Data Breach.** If personal data has been lost, accessed unlawfully etc libraries must inform authorities of the breach within 72 hours. People affected must also be told as soon as is practicable after the event took place unless the personal data has been encrypted.

---

[1] Prepared for IFLA by Benjamin White, British Library, 29 July 2017. This briefing does not constitute legal advice and should purely be treated as guidance in thinking about how to apply new European data protection rules. It may also be of interest to libraries in countries reflecting on similar reforms, or who may be processing personal data about European Union citizens.

[2] A patron's consent must also be a positive, tangible and affirmative step. Silence cannot be inferred as consent or used a legal basis for using someone's personal information.

[3] This is a process where most identifiable features in data are replaced by an artificial identifier or pseudonym. If necessary the "key" to the pseudonym can be held elsewhere.

[4] In data protection law, this is called a "privacy impact assessment". You can find the official UK guidance on how to achieve this at the following link: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

- **Rights of Library Patrons.** People will have the right to be informed free of charge as to what information you hold on them and for what purpose it is being used. They also (alongside a number of differing rights) have the right to be supplied a copy in electronic form of the data you hold on them, and to require in many cases that data you hold on them is rectified, removed or deleted from your systems.
- **Data Protection Officer.** All public authorities, which in many if not all member states will include public, national and university libraries, must appoint a data protection officer. A data protection officer can be shared with other organisations (for example with local government), but must be registered with the national data protection authority. Legally this person must report to senior management and must have no conflict of interest in performing this role. For example, they should not be part of an IT Department, or report to a Chief Technology Officer.

Actions for All Libraries:

- Establish your legal basis for processing personal data wherever this is done across your organisation. For example, identify where you rely on consent to process personal data, where you process data based on a legal requirement, or as part of your public task as a public body. Establish for all your activities if your grounds for processing personal data are either based in legislation, your role as an organisation performing a public task, and / or based on consent from the library patron.
- If relying on consent for using personal information: firstly ensure that your terms and conditions that relate to using patrons' personal data are easily accessible (e.g. short) and understandable to a layman of any age. Secondly, ensure that they clearly explain exactly what you are using a patron's personal data for in plain language. Finally, make sure that the consent is a positive action – using pre-populated tick boxes for example are not valid.
- All libraries must have written records outlining the purpose for using personal data, the categories of personal data stored[5], time limits for deleting personal data, technical and organisational measures to protect personal data etc. Upon request such information must be supplied to the appropriate data protection authorities.
- In addition to the above ensure that:
    1. You review your processes relating to handling personal data and ensure you can comply with obligations such as supplying or removing personal data, and are able to explain precisely how you are using a patron's personal information.

[5] i.e. Whether the data held is personal data or sensitive personal data – this includes personal data relating to ethnicity, political or religious beliefs, sex life, health matters, trade union membership and genetic / biometric data. You should also list whether the personal data includes patrons, employees, contractors etc.

2. You employ “privacy by design” principles mapping out current processes relating to personal data, and when you introduce new processes (like a new IT system) you evaluate how this will impact on the personal data you hold.

Are there any specific exemptions from the law for news and collections of a political nature, archives and research activities?

Yes there are, but they are not automatic. You or your library organisation should engage with policy makers and / or the national body that oversees data protection law to clarify whether these exemptions from the regulations (see below) will be introduced into your country or not. If not, we recommend that you request they are.

a) Freedom of Expression and Information Exemptions

The regulation allows member states to introduce very wide exemptions for freedom of expression and information purposes that would reduce many of the burdens the act imposes on libraries. In the section in the regulation referring to freedom of expression and information it specifically mentions news, broadcast and press libraries. However given that many libraries hold news and broadcast content, and archives of a political nature which are important for freedom of expression, the regulation provides explicit grounds for exempting many libraries and archives from the obligations in the regulation on the basis that libraries and archives play an important role in guaranteeing freedom of expression. You should encourage your government to extend freedom of expression exemptions to the activities of libraries and archives.

b) Archival Exemptions

The regulation provides more limited exemptions for organisations “archiving in the public interest”, though some of these are not mandatory so Member State can choose to pass them into law or not. However in order to enjoy these exemptions, an organisation archiving in the public interest must have a **legal obligation** to “*to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest.* “ You should ask your government if unclear, as to whether all types of libraries and archives have a legal obligation to perform these activities, or whether a new legal underpinning will be required.

c) Research Exemptions

The regulation also provides non-mandatory exemptions for scientific or historical research purposes, as well as using personal data for statistical purposes. As with the archiving exemptions these are not mandatory, so a member state can decide whether to pass them into law or not.

Further resources: www.eugdpr.org