A Practical Guide to Data Protection for Information Professionals

Naomi Korn and Carol Tullo
on behalf of NKCC

© NKCC 2018. All Rights Reserved. www.naomikorn.com The information contained within this document is for guidance only. Please refer to a suitably qualified legal profession for legal advice.
Contents

Introduction 3
What is data protection and why is it important? 4
Types of personal data 5
What is processing? 6
What is GDPR? 6
What are the legal grounds for processing? 7
Key definitions 8
Am I the right person for the role of DPO in my organisation? 10
What rights do individuals have and what does my organisation need to do? 11
FAQs for library and information professionals and their organisations 12
Checklist 16
CILIP is the UK's Library and Information Association. Our role is to help information professionals develop the skills they need to future-proof their careers and deliver real impact in their work. For more information about how we can support you in your career, visit cilip.org.uk.

As a library and information professional, you know the importance and value of information management and data security as you deal with sensitive personal data in the course of your day-to-day responsibilities. Our aim is to provide an overview and introduction to the principles of data protection compliance to refresh your expertise in the subject and to reinforce your position as the information specialist in your organisation.
Data protection principles have already been part of our professional information world for 20 years, with our current focus on the strengthened data protection regime from May 2018. This ensures a standard approach with the General Data Protection Regulation (GDPR) becoming part of UK law.

Respect for information that relates to a living person, who can be identified from that data, or from that data when combined with other information you hold, guides you as an information professional. There are six principles that you need to follow in processing such information:

1. It is lawful, fair and transparent
2. It is specific, explicit and legitimate
3. It is adequate, relevant and not excessive
4. It is accurate and kept up to date
5. It is kept for no longer than necessary
6. It is processed securely

How can I remember them?
This simple mnemonic may help:

Legal grounds for processing must always be established
In accordance with the rights of the individual
Beware sharing or using personal data beyond the initial legal grounds
Robustly secure access to personal data and keep it safe
Adequate, relevant and not excessive amounts of personal data can be kept
Retain personal data only as long as necessary
You must take responsibility for why, how, where and for how long you process personal data

What is data protection and why is it important?

Don't listen to scare-mongers. Yes, GDPR is a step up from current data protection laws, and there is no magic bullet. The Data Protection Act 2018 is about embedding long term systematic “privacy by design” processes and policies within organisations. There is no ICT system that solves it!
Key points to remember:

- We are not just talking about data held on computer but also paper files.
- If your organisation is already data protection compliant then it is in a good place to meet its legal obligations regarding the storage and use of personal data.
- There is stronger legal protection for more sensitive information.

### Types of personal data

Personal data is information about living identifiable individuals. Within the context of your activities this will include:

- Names, addresses and contact details about library members
- Personal information about staff, contractors, volunteers, students, interns and visitors
- Personal information held on Library Management Systems
- Expressions of opinion about a person
- Membership, mailing and events lists
- Computer's IP address
- Posts on social networking sites
- Medical information
- Photographs
- CCTV footage
- Fingerprints and/or retinal scans
Sensitive personal data additionally contains information that tells you about private aspects of an individual’s life such as racial origin, political opinions, health and sexual life, genetic and biometric data. There is a presumption that this data is private, open to misuse and therefore needs to be treated with greater care than other personal data.

Key points to remember:
- There will be other legal, regulatory, ethical and policy frameworks relating to personal information with which you must comply.
- Context is everything, so data placed with other data, can create a profile of a living identifiable individual.

**What is processing?**

This is defined very widely and includes collection, storage, use, recording, disclosure or manipulation of data whether or not by automated means. You will be processing personal data in a number of ways about library users, and in some cases, this data might include sensitive data such as users who have specific learning needs or physical disabilities.

**What is GDPR?**

The General Data Protection Regulation is a legal act of the EU that is immediately enforceable in law across the EU simultaneously on May 25, 2018. It further harmonises data protection rules across the EU, enhancing privacy rights for individuals and increasing obligations on those that hold data. It applies to all organisations processing personal data which have an establishment within the EU and also those organisations which operate outside the EU but offer goods or services to, or monitor the behaviour of, individuals in the EU. The aim of GDPR is greater transparency, enhanced rights for citizens and increased accountability.
Data Protection law applies to print and digital forms of personal data. Know what you have, why and where it is stored. Decide if you should keep it or not, and if so, make sure you plan how you keep it secure.

**The key changes are:**
- Greatly enhanced rights for individuals
- Increased accountability and transparency by organisations
- Visibility of Data Protection Officer role in organisations
- Greatly increased sanctions for data breach
- Stronger conditions for consent

**Key points to remember:**
- GDPR applies across the EU from 25 May 2018
- In the UK, GDPR will become part of the Data Protection Act 2018.

---

**What are the legal grounds for processing?**

Without grounds for processing, or a lawful basis for processing, your organisation cannot process data legally. The most appropriate lawful basis will depend on the Personal Data being processed and the purposes for processing.

**There six different grounds for processing:**

**Consent** – the individual must give their consent freely. It must be opt in, unambiguous, specific and informed with no conditions. Note that children under the age of 13 require particular protection and there are additional requirements to obtain verified parental consent. Example: pre-ticked boxes for signing up to mailing lists will not be acceptable.

**Contractual** – processing is necessary for the performance of a contract or agreement to which the individual is party or is required prior to entering into a contract. Example: staff working in a library are required to keep records of all those who have authenticated access to specific journals as part of their licence obligations.

**Legal basis** – processing is necessary for compliance with a legal obligation to which the individual is subject. Example: employer passing salary details to HMRC or the fulfilment of pension obligations.

“The new regime is an evolution in data protection, not a revolution. It demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. GDPR is building on foundations already in place for the last 20 years.”

If you can’t find a legal justification for processing personal data, delete or destroy. Otherwise it’s your risk.

**Vital interests** – processing is necessary to protect the vital interests of the individual or of another person. Example: schools need to keep records of pupils with medical or allergy requirements.

**Public interest** – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. Example: local authority funded public libraries are able to process personal data for the purposes of lending books to members of the public because that is what they are being funded to do.

**Legitimate interests** – processing is necessary for the purposes of the legitimate interests of the organisation or a third party. The data is used in ways which people would reasonably expect. Example: Universities capture student data and statistics in the course of their period of study at that university.

**Key points to remember:**

- Identifying the ground for processing personal data is always your starting point.
- The ground must be reasonable, proportionate and targeted.
- Where personal data is collected people must always be told of the legal ground for processing.
- Document your decision and include it in your Privacy Statement or Notice to meet your accountability and transparency obligations.
- If you process children’s data or think you might in future, then design your processes with this in mind.

**Key Definitions**

Within your organisation, there will be levels of accountability regarding your data protection obligations.

**Data controller:**

Any person, or organisation, who makes decisions about how and why data is processed. A data controller must be a person recognised in law and they are responsible for compliance. Example: a self-employed consultant; Head of Library Services; Chief Executive of a public body.
**Data processor:**
Any person, or organisation, who acquires, records and processes personal data on behalf of the controller. Example: a library management system run by an external software company processes library user information on behalf of a library. The library is the controller and the software company is a data processor.

**Data subject:**
A living person who is the subject of personal data. The individual who has enhanced rights under data protection law.

**Data breach**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Organisations are required to report a data breach that creates a risk to the rights and freedom of the individuals concerned, to the Information Commissioner’s Office (ICO) within 72 hours of the breach occurring or when made aware of the breach. If the individuals are at high risk of potential harm, then they must also be notified. Example: A computer account is hacked, and data listing contact details is accessed or a member of staff takes unencrypted data home on a memory stick and loses it.

**Data Protection Officer (DPO):**
This is the role in an organisation which has responsibility for ensuring that personal data is protected and that the organisation is compliant with the legislation. There should be a degree of independence so the DPO reports direct to the highest management level of the organisation as a part of the organisation’s governance. The DPO:

- Monitors compliance with the Data Protection Act 2018
- Has suitable expertise or experience
- Is the primary Data Protection contact point in the organisation
- Assists with Data Protection Impact Assessments
- As the information professional in the organisation, may hold the asset register and records of the organisation as the central point for ensuring that the organisation is compliant
- Understands and advises on a risk-based approach to data processing in their organisation
Make sure you understand your obligations as a Data Controller when others are processing personal data on your behalf. Always ensure you have robust contractual agreements with your third party data processors.

- Ensures robust breach investigation takes place, internal reporting procedures and outcomes are recorded
- Where appropriate, registers with the ICO www.ico.org.uk

Key points to remember:
- The organisation is the Data Controller and is responsible for compliance. The senior management team are advised by the DPO, but ultimate responsibility rests with the Data Controller
- An organisation can be both a data controller and data processor even where they may appoint third parties to carry out elements of data processing on their behalf, such as Cloud Computing services
- The DPO remains independent for the purposes of carrying out their tasks which may be wider than data protection
- Organisations where the core activity is large scale data processing and public authorities and bodies have a mandatory requirement for a DPO.

Am I the right person for the DPO role in my organisation?

The requirements for a DPO are:
- Professional and expert knowledge of data protection though this can be as part of other relevant experience within the information field.
- Employed in the organisation or with a service contract to fulfil the role.

As a librarian/information professional, you will often be best placed to provide your organisation with data protection expertise. You will demonstrate that you are:

1. Qualified and/or experienced in managing information and already have a broad understanding of legal compliance issues such as information management, data protection and/or copyright.
2. In a position to have broad oversight of your organisation’s activities and those involving the processing of personal data.
3. Well placed in your organisation to provide neutrality in the role of DPO and not to present any conflict of interest.

4. CILIP members will have continuing access to data protection updates via training, CILIP’s Virtual Learning Environment (VLE), CILP networks and other professional initiatives.

5. Best placed to carry out Information Asset Audits, amend and refresh existing policies and develop new policies.

6. Already the guardians of related Records Management Policies and/or Retention Schedules.

7. Knowledgeable about all data aspects of your business sector and of the organisation

8. In the case of a public authority or body, you will have a sound knowledge of the administrative rules and procedures of the organisation.

Key points to remember:

- Not every organisation needs a designated DPO, but it is advisable to have a named person in the role who carries out the responsibilities and is a key point of contact

- A DPO can be shared among linked organisations. Example: departments within a local authority, a library within a wider university group, or a group of schools within an Academy Trust.

What rights do individuals have and what does my organisation need to do?

There are strengthened rights for individuals over their data that you are processing. They can request an organisation to make changes in how their data in handled and you must respond promptly should a request be made. Your organisation may be unlikely to receive such requests on a regular basis, so the important thing is to be able to recognise them should you receive one:
Top Tip #9
Embed clear guidance about data protection into staff awareness and engagement. It's everyone’s responsibility.

- Right to be informed – communicate clearly and use plain language in all your external messaging
- Right of access – have in place processes to respond to requests for what information you are holding (Subject Access Requests)
- Right to rectification – ensure you correct inaccurate information in the data you are processing without delay
- Right to erasure – you may be required to delete the data and stop processing it or publishing it (often called the Right to be Forgotten)
- Right to restrict processing – where the accuracy or lawful processing is challenged then temporary limits on the processing are required
- Right to data portability – you may be asked to provide the personal data you hold, securely and in a machine-readable format, so it can be moved, copied or transferred to be used across different services
- Right to object – ensure you have the right consents in place for activity such as direct marketing
- Rights related to automated decision making – if there is additional profiling based on the data you hold then an individual can object

FAQs for library and information professionals and their organisations

I have a membership list from 2010, do I need to ask for fresh permission to send mail-outs?
Yes, you will need to ensure that you have sought consent for any processing of personal data. This is an opportunity for you to update your membership lists, reach out to existing members and demonstrate that you take data protection and their privacy seriously.

If library members’ details have been updated and/or they cease to be members, do I need to update our Library Management System (LMS)?
Yes, your LMS will need to reflect such changes. Data subjects can also request that their personal data is erased, and your LMS needs to have this functionality.
What should we do about suppliers, particularly if we use Cloud Computing services that are not based in the European Economic Area?

You must ensure that you put in place contracts with all your suppliers which clearly define their responsibilities in terms of your obligations under the Data Protection Act 2018. If you are subject to their terms and conditions, you will need to satisfy yourself that they do not share personal data, they keep it secure and if they use any sub-contractors or third parties to perform their duties, they are also subject to rigid data hygiene rules. As a Data Controller, if you are not satisfied, you should use another provider.

How long should we keep details about library members?

Personal data about library members should be kept only as long as you need it. You should record retention periods on a retention schedule, and make sure that you factor in other legal obligations or organisational policy requirements that you may have, into decisions about how long you retain data.

Can I keep historic data, or should I purge it?

Unless you have legal grounds for processing or you are required to keep such data, you should delete it.

Key points to remember:

- The Data Protection Act 2018 is a small step up if your organisation or library is data protection compliant already
- Know your new obligations as Libraries are likely to be both data controllers and data processors
What do I need to do next?

The ICO has published 12 Steps to help you in your journey towards compliance with your requirements under the Data Protection Act 2018.

Under the new obligations outlined within the Data Protection Act 2018, you will also need to embed a “Privacy by Design” approach into everything that you do. As you start a new project build data privacy and respect for personal data into the planning from the outset. You can do this by embedding your data protection responsibilities by using the NKCC Compliance Framework [www.naomikorn.com](http://www.naomikorn.com) which views compliance as a series of operational and strategic interventions built upon wide reaching data protection awareness and training and supported by robust governance and commitment.
Key points to remember:

- Take responsibility for your data activities and for those who do it for you
- Know what you collect, why and for how long you keep it
- Take this opportunity for a deep data clean
- Document your processes and policies to evidence your sound housekeeping of data
- Treat personal data as you would want your data to be treated by others

Where can I find out more about Data Protection?

- www.ico.org.uk
- www.dpnetwork.org.uk
1. Review all the data you are holding
2. Identify bases for processing it
3. Document your processes and procedures
4. Check compliance with your third party contractors and those that process data on your behalf
5. Set out your breach process
6. Decide how to handle requests from individuals
7. Appoint a DPO
8. Refresh your Privacy Notice or Statement
9. Raise awareness in your organisation