# Data Protection Elearning Module

## By Naomi Korn, Naomi Korn Associates

### Setting the Scene

The General Data Protection Regulation (GDPR), effective from 25 May 2018 and incorporated in the Data Protection Act 2018, harmonises data protection rules across EU member states. It applies to data processing carried out by individuals and organisations operating within the EU, but also applies to organisations outside the EU that offer goods and services to EU citizens. The GDPR significantly enhances the rights of data subjects in the processing of their personal data and strengthens the current system. The Data Protection Act 2018 controls how personal data is used by organisations, businesses or the government.

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.

### Aim of the Module

The aim of this elearning module is to provide you with an overview and introduction to the principles of data protection compliance to refresh your expertise in the subject, build your confidence and professionalism and to reinforce your position as the information specialist in your organisation.

### What is Data Protection and why is it important?

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.

### True or False?

1. Personal Data can only be kept for a maximum of 5 years?

   False.
   You should keep it as long as you need, and outline clearly in a retention schedule the different lengths that you are storing personal data for.

2. Data Protection Laws override other legal obligations?

   False.
   Data protection laws dovetail into other statutory and regulatory obligations. In the case of Freedom of Information, there is an exemption that if an FOI request contains personal. Data, the information has to be redacted.

3. It is vital that information professionals make every effort to keep personal data updated where possible, and to use technological and operational means to protect it against potential data breaches.

True.

Key points to remember:

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

**What is Personal Data?**

Personal data is information about living identifiable individuals.

PLEASE SELECT WHICH OF THE FOLLOWING ARE PERSONAL DATA?

- 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
- **General factual opinions X**
- **Anonymised data X**
- Expressions of opinion about a person
- Membership, mailing and events lists
- Computer's IP address
- Posts on social networking sites
- **Information about a deceased person with no connection to a living identifiable individual X**
- 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.

PLEASE SELECT WHICH OF THE FOLLOWING ARE SENSITIVE PERSONAL DATA?

- 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?**

**How is GDPR different?**

This new framework builds on and enhances existing data protection law. The key changes are:

- Greatly enhanced data subject rights
- An increased requirement for accountability and transparency by data controllers
- Visibility of the Data Protection Officer role in organisations
- Greatly increased sanctions for data breaches
- 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 6 different grounds for processing:

**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.

**Legal basis** - processing is necessary for compliance with a legal obligation to which the individual is subject.

**Vital interests** - processing is necessary to protect the vital interests of the individual or of another person.

**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.

**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.

**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.

**Please tick the lawful grounds for processing which might apply in a library context?**

**True: Contractual** - 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.

**True: Legal basis** - Employer passing salary details to HMRC or the fulfilment of pension obligations.

**True: Vital interests** - Schools need to keep records of pupils with medical or allergy requirements.

**True: Public interest** – 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.

**True: Legitimate interests** - Universities capture student data and statistics in the course of their period of study at that university.

**True: Consent** - Pre-ticked boxes for signing up to mailing lists will not be acceptable, and information management staff must ensure that consent is opt in, clearly communicated and also recorded on Library Management Systems.

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.

**Please choose the correct definition from one of the definitions provided:**

| | **Data Protection Term** | **Definitions:** |
|---|---|---|
| 1. | Data controller | **1. Any person or organisation who makes decisions and determines how and why data is processed**<br>2. Any person or organisation who is responsible for an IT system<br>3. Any person who enters data into an IT system |
| 2. | Data processor | 1. Any person who is responsible for structuring the way data is entered in a database<br>**2. Any person or organisation who collects, stores, discloses or processes personal data on behalf of the controller**<br>3. Any person or organisation who acquires, records, retrieves and makes data available to others |
| 3. | Data | 1. Information that is held on websites<br>2. Structured information that is held on a computer or is intended to be held on a computer<br>**3. Information that is held in a manual filing system or is processed by a machine** |
| 4. | Data subject | 1. Any person, living or dead, to whom the data relates<br>**2. The living person to whom the data relates**<br>3. The subject or contents of a database or filing system |

| | | |
|---|---|---|
| 5. | Data Breach | **1. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.**<br>2. Any breach of data<br>3. Loss of digital content |

**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. This means that the library must ensure that the suppliers of the library management system are compliant with its data protection obligations, keeping data safe, not sharing with third parties or re-using it and alerting the library of a suspected data breach as promptly as possible.

**Data:**
Information that is held in a manual filing system or is processed by a machine. In a library context, this will include digital content, as well as paper files like library catalogue files.

**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.

<u>Key points to remember:</u>

- The Data Controller is responsible for compliance and this cannot be delegated by the senior management team. They are advised by the DPO but the organisation is the responsible 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
- 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.

**The Role of a Data Protection Officer**

**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
- 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 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 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:

- 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 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

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 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

**Checklist:**

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
10. Get senior buy-in as responsibility sits at that level

**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***