INDEPENDENT BOOKSELLERS FORUM

Guides to Practical Bookselling

General Data Protection Regulation (GDPR)

Table of Contents

Introduction

Currently, the Data Protection Act 1998 is the main law which lays out how organisations and businesses should treat the personal data which they handle. Many of you will be familiar with the Act and will already be up to scratch with meeting the requirements.

However, on 25th May 2018, the EU is introducing a new data protection regulation: the General Data Protection Regulation (GDPR). The UK government has confirmed that Brexit will not affect this: UK companies will still need to adopt the GDPR.

This guide is designed to give booksellers an overview of the requirements of the GDPR and to give some practical tips on how to meet these requirements. Some of the requirements are very similar to those of the Data Protection Act 1998, some are more thorough enhancements and some are completely new. Key changes or additions will be marked with this symbol:

If you have any questions about this guide or any comments on how to improve this guide please do email pippa.halpin@booksellers.org.uk.

Why it matters

- The GDPR is introducing much stricter fines for companies who are found wanting. You can be fined up to €20,000,000 or up to 4% of your turnover (whichever is greater).
- The consequences of a failure to protect your data can be very damaging to your business' reputation. In severe instances, it could lead to the closure of your business.
- The consequences of a failure to protect your data can be very damaging to the customer or staff member whose data has been compromised. It can negatively affect their life for many years. The ultimate purpose of data protection law is to protect them (the data subject) rather than you (the data processor).

Jargon

We've tried to keep this guide as jargon-free as possible but sometimes we think it's necessary to copy some of the terms in the GDPR, to keep things precise and concise.

These terms are:

Personal data – data which relates to a living individual who can then be identified by this data/by combining this data with other accessible data (eg name, home address, email address, card details, online identifiers such as an IP address etc)

Sensitive personal data/special categories of personal data – racial and ethnic origins, religious beliefs, trade union membership, physical or mental health, sexual life, alleged or proven criminal offences, biometric data

Processing data – obtaining, recording, holding, organising, adapting, consulting, accessing, disclosing, transferring, erasing or destroying data

Data controller – a person who decides why and how personal data is processed (eg the owner of the bookshop)

Data processor – a person who processes personal data on behalf of the data controller (eg the manager of the bookshop, a shop floor sales assistant)

Data subject – a person who is the subject of the personal data (eg the customer or an employee)

Compliance – meeting the requirements of the law/regulation

Subject Access Request (SAR) – when a data subject requests to see all of the personal data you processing about them (whether electronically or on paper)

DPA – Data Protection Act 1998

GDPR – General Data Protection Regulation

ICO – Information Commissioner's Office

PIA/DPIA – Privacy Impact Assessment/Data Protection Impact Assessment

GDPR principles

The data protection principles of the GDPR are very similar to those in the DPA.

GDPR change

The key addition is the **new accountability requirement**: you have to **show how** you comply with the principles.

Personal data shall be:

(a) processed **lawfully, fairly** and in a **transparent** manner in relation to individuals;

(b) collected **for specified, explicit and legitimate purposes** and **not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

(d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) **kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

"**the controller shall be responsible for, and be able to demonstrate, compliance with the principles.**"

Key new areas to consider

GDPR change

- You need to **work out AND document the legal basis for processing** the various types (eg contact details, payment details, employment details) of personal data you handle. The ICO's *Overview of the GDPR* has a comprehensive table of legal bases.

  For most booksellers, the legal basis is likely to be:
  - either 'consent of the data subject' (eg a customer agrees to give you their email so they can sign up to your book club)
  - or 'processing is necessary for the performance of a contract with the data subject' (eg you need to take credit card details in order for a customer to buy a book)

GDPR change

- **'Consent'** under the GDPR requires some form of **clear affirmative action**. Silence, pre-ticked boxes or inactivity don't count. It must also be **verifiable**.

  So you should amend any paper and online forms which ask for consent, to make sure they are 'opt-in' and not 'opt-out'. You should also keep a record of how and when consent was given. If your current practice doesn't meet the GDPR standard, then you'll have to get fresh (verifiable, clear and affirmative) consent from people if you want to keep using their personal data after May 2018.

GDPR change

- If you process **children's (under 16) personal data**, you need to make sure:
  - your privacy notice is easily understood by children
  - you have the parent/guardian's consent if you offer the child online services

Individuals' rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The right to be informed

You have to explain how you and why you are using someone's personal data. Typically, companies provide a '**privacy notice'** when they are collecting the data (this could be on your website, on a paper form, etc).

The ICO's *Overview of the GDPR* and *Privacy Notice Code of Practice* have a comprehensive list of exactly what the GDPR says should be included in your privacy notice: **you should check carefully that your privacy notice covers all of these areas as some are additional to the DPA requirements.**

GDPR change

The right of access

Similarly to the DPA, under the GDPR individuals have the right to have:

- confirmation that their data is being processed
- access to their personal data
- other additional information (which ought to be covered by your privacy notice)

This is so that they can check that you are handling their personal data legally.

If someone requests access to the personal data you hold about them this is referred to as a **'Subject Access Request'**. **You have to provide this information free of charge** (under the DPA you could charge £10 for a Subject Access Request) and **as quickly as possible** (usually within one month at the latest). If they request the information electronically, then **you have to provide the information in a commonly used electronic format** (eg Excel spreadsheet, Word Document, etc).

GDPR change

GDPR change

The right to rectification

Individuals are entitled to have **personal data rectified if it is inaccurate or incomplete**, usually within one month. If you have shared the personal data to **third parties, you must inform the third party** of the rectification where possible.

The right to erasure

Individuals are entitled to **request the deletion or removal of personal data** where:

- the personal data is no longer necessary for the purpose for which it was originally collected
- the individual withdraws consent
- it was or will be processed illegally
- it relates to offering online services to a child

If you have shared the personal data to **third parties, you must inform the third party** of the erasure where possible.

The right to restrict processing

Individuals have a right to block processing of their personal data: you can then still store the data, but you mustn't do anything with it.

If you have shared the personal data to **third parties, you must inform them** of the restriction where possible.

The right to data portability

GDPR change

Individuals are entitled to **obtain and reuse their personal data for their own purposes across different services**. This allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindering the usability of the data.

GDPR change

You have to provide the information in a structured, commonly used, machine readable electronic format (eg Excel spreadsheet, Word Document, etc) so that other organisations can use and extract the data. You must provide this **free of charge** and **as quickly as possible** (usually within one month).

The right to object

Individuals are entitled to object to **direct marketing** (and some other things not obviously relevant to booksellers).

GDPR change

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. **If your direct marketing is carried out online, then you must offer a way for individuals to object online** (eg via your website).

Rights related to automated decision making and profiling

The GDPR (like the DPA) provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

You should **identify whether you use any automated decision making when processing personal information** (for most independent booksellers, this will be unlikely). If you do, in some instances the individual will have a right to obtain an **explanation of the decision** and **challenge it**, as well as obtain **human intervention**.

Accountability

The GDPR emphasizes the **principles of accountability and transparency** more explicitly than the DPA. You are expected to put into place **comprehensive but proportionate measures** to look after your data. Good practice tools such as **privacy impact assessments** are now legally required in certain circumstances. Practically, this is likely to mean more policies and procedures for booksellers.

What is the new accountability principle?

GDPR change

You have to **demonstrate that you comply** with the GDPR data protection principles.

How can I demonstrate that I comply?

- **Implement technical and organisational measures** (eg regularly train staff in your data protection policy, regularly delete out of date personal data, regularly change computer passwords)
- **Maintain relevant documentation** on data processing (eg document when and how you have audited your data, document your staff data protection training schedule/content/outcomes)
- **Appoint a data protection officer** (for some companies this is a requirement, but is generally encouraged even when not required)
- **Use privacy impact assessments** where appropriate (see later section)

In more detail…

Maintain relevant documentation: what do I need to record?

GDPR change

- Name and details of your organisation (the data controller and data processor)
- Purposes of processing the personal data

- Description of the categories of individuals (data subjects) and the categories of personal data
- Categories of recipients of personal data (eg banks, suppliers)
- Details of any transfers to third countries (eg servers outside the EU which store your electronic data and emails)
- Retention schedules (i.e. how long you will keep the data for)
- Description of technical and organisational security measures (eg how often you enforce changing of computer passwords)

Appoint a data protection officer: am I *required* to have one?

GDPR change

- Yes, if you are a public authority
- Yes, if you do large scale systematic monitoring of individuals (eg online behavior tracking)
- Yes, if you carry out large scale processing of special categories of personal data or data relating to criminal activity

Many booksellers will not fall into the above categories. However, if you choose not to appoint a data protection officer, you must ensure that your organisation has sufficient staff and skills to still discharge your obligations under the GDPR.

Further GDPR guidance on data protection officers is available here: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

Use privacy impact assessments: why, when, what?

Privacy impact assessments (PIAs) are **a tool to help you identify and minimise the privacy risks of new projects or policies**. They help you ensure that potential problems are identified at an early stage, when addressing them will be simpler and less costly. Conducting a PIA does not have to be complex or time consuming.

GDPR change

You **must** carry out a PIA when **using new technologies** or when processing data on a large scale. They are a useful tool for any new project though (eg if you decide to change the way you process card details or customer orders).

The ICO's PIA code of practice has some **screening questions to decide if a PIA is necessary**, as well as a **PIA template** and **clear steps** for the process: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Breach Notification

GDPR change

The GDPR introduces a requirement that all organisations will have **a duty to report certain types of data breach** to the ICO (for UK booksellers) or the Data Protection Commissioner (for Republic of Ireland booksellers) and, in some cases, to the individuals affected.

A personal data breach is a **breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**.

You only have to **notify the ICO/DPC** of a breach when there is a **risk** to the rights and freedoms of individuals (eg damage to reputation, financial loss, loss of confidentiality with significant detrimental effect, discrimination). You only have to **notify the affected individuals** when there is a **high risk** to the rights and freedoms of individuals.

UK booksellers: Relevant breaches must be reported to the ICO **within 72 hours** of you becoming aware of the breach. You can report breaches here: https://ico.org.uk/for-organisations/report-a-breach/

Irish booksellers: Relevant breaches must be reported to the Data Protection Commissioner **within 72 hours** of you becoming aware of the breach. You can report breaches here: https://www.dataprotection.ie/secur-breach/

You should ensure you **have an internal breach reporting procedure** in place and **train your staff** so that they understand what constitutes a data breach.

Transfer of data

GDPR change

The GDPR imposes **restrictions on transferring personal data outside the EU** (at the time of writing this guide, there is no clear guidance from the ICO on whether the UK should be treated as inside the EU for this purpose).

Many booksellers will not find this will affect them, although you should check (and record) that any non-EU companies storing your data (eg if their servers are in the US) are compliant with the 'adequate safeguards' required by the GDPR.

The ICO's *Overview of the GDPR* has further details on this area if you think it is relevant to you.

12 steps to take now

Based on the above information and changes, at a minimum you should:

1. **Make all key people in your business aware of the impact the GDPR will have on your business**
   This may involve adding data protection to your company's risk register, if you have one. You will need to make it clear that preparing for the GDPR should not be left until the last minute.

2. **Document what personal data you hold, where it came from and who you share it with**
   This will help you comply with the accountability principle, as well as the right to access, the right to rectification and the right to erasure.

3. **Review your current privacy notice and make the necessary changes**

4. **Check that your procedures cover all the above rights that individuals have**
   This will include documenting how you will delete personal data and how you will provide data electronically and in a commonly used format.

5. **Update your subject access request procedure**
   This will include planning how to handle requests within the new timescales.

6. **Document your legal basis for processing the various types of personal data you handle**
   This will include ensuring this legal basis is explained in your privacy notice.

7. **Review how you are seeking, obtaining and recording consent and then make the necessary changes**
   This will include ensuring that consent is now clear, verifiable and affirmative: it cannot be inferred from silence, pre-ticked boxes or inactivity.

8. **Think about how to verify children's ages and gather parental consent for processing their personal data**

9. **Ensure you have the right procedures in place to detect, reports and investigate a personal data breach**
   This may involve assessing and documenting which types of data breach would need to be reported to the ICO or the individuals affected

10. **Work out how and when to implement a PIA**

11. **Designate a Data Protection Officer (if required) or someone to take responsibility for data protection compliance**
    This will involve ensuring they have the knowledge, support and authority to take on the responsibility.
    This may involve training and/or tweaking your organisation's staffing structure.

12. **If you operate internationally, you will need to determine which data protection supervisory authority you come under.**
    Many booksellers will have their central administration (i.e. the place where decisions about processing personal data are taken) in the UK, in which case your supervisory authority is the ICO https://ico.org.uk.
    If your bookselling business has its central administration in Ireland, your supervisory authority is the Data Protection Commissioner www.dataprotection.ie.
    The ICO has confirmed with the BA that if your organisation's central administration is in the UK but you also have Irish branches, then your supervisory authority is still the ICO.
    If you are unsure, give a quick call to the ICO (0303 123 1113) to check with them.

Information Commissioner's Office (ICO) Guidance on the GDPR

The Information Commissioner's Office is the UK's independent body set up to uphold information rights. Their role is to uphold information rights in the public interest. Their work covers, amongst other legislation, the Data Protection Act 1998 and the upcoming GDPR.

Their website is https://ico.org.uk and the full version of the Data Protection Act 1998 can be found here: https://ico.org.uk/about-the-ico/what-we-do/data-protection-act/.

Looking ahead to the introduction of the GDPR in May 2018, the ICO have added a new, regularly updated section to their website, dedicated to helping organisations understand the GDPR and put it into place: https://ico.org.uk/for-organisations/data-protection-reform/.

Much of the information in this guide is a summary of the information on the ICO website. The following material that they have produced covers the topics in this guide in more detail:

Overview of the GDPR: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

GDPR 12 steps to take now: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Privacy notices code of practice: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Privacy impact assessment code of practice: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Use of the ICO material