General Data Protection Regulation (GDPR) guidance
Part 1

Summary

Data Protection law is changing with the introduction of the General Data Protection Regulation (GDPR) on 25 May 2018. This is the biggest change to data protection legislation since the Data Protection Act (DPA) in the late 1990s.

This guidance for Local Optical Committees (LOCs) to help them understand the changes and actions that they need to take. Practices should refer to the guidance from the Optical Confederation issued on the 15 December 2017 http://www.opticalconfederation.org.uk/downloads/data-protection-and-gdpr-guidance--final.pdf.

Overview

Most of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA) and so most of your approach to compliance will remain the same. However, there are some new elements and some enhancements, so there will be some changes to be made.

The Data Protection Bill is still going through the UK Parliament and the Information Commissioner's Office (ICO) is still updating its guidance. This will be finalised when the bill has been passed and full details confirmed. LOCSU along with the OC will issue any further guidance as required.

What's new

The definition of personal data has been substantially expanded under the GDPR. Anything that counted as personal data under the DPA also qualifies as personal data under the GDPR and it now also includes cultural records, health records and online identifiers such as IP addresses.

The main responsibility created for organisations is compliance with GDPR principles, which are themselves, an expansion of DPA principles. Personal data needs to be:

- processed lawfully, fairly and transparently.
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- adequate, relevant and limited to what is necessary for the purpose it was collected for
- accurate and up to date.
- kept in such a way that it permits identification of the data subject for no longer than necessary.
- processed so as to ensure appropriate security of personal data.

In addition, the GDPR creates rights for individuals and it is a further responsibility for organisations to respect these rights:

- The right to be informed.
- The right of access.

- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

See table 1 for more detail on these eight rights.

Another difference between DPA and GDPR is the addition of an accountability requirement. Not only do organisations need to comply with their responsibilities under GDPR, they will need to show how they do so. Various records therefore have to be maintained in order to demonstrate compliance including consent, legal basis for processing and data retention policies.

GDPR also introduces a duty on organisations to report certain types of data breach within 72 hours.

Finally, the GDPR imposes a restriction on transferring personal data outside the EU or to international organisations.

Next steps

Understanding the information you need to hold, what is personal identifiable information, where you store it and how you use it is key. LOCs must understand what they do, and don't, need to store and process, where they're allowed to store it, and what they're allowed to do with it. Your members should also develop increased awareness of the information you hold, why you hold it, what you intend to do with it, and what to do if they object to that.

Ensure that this information is read by the key people on the LOC.

Key steps

- Document all the personal data that you hold on paper and electronically.
- Identify and document the lawful basis for processing the personal data held. See table 2.
- Review your current privacy notice and plan any changes that need to be made in light of GDPR.
- Check your procedures to ensure that they cover all the rights that individuals have.
- Ensure that your procedures for handling requests for personal data are up to date and take into account the new GDPR requirements.
- Review how you seek, record and manage consent and whether you need to make any changes. It may be appropriate to seek fresh GDPR-compliant consent.
- Review the methods you use to keep data secure and update them if necessary.
- Ensure that only the data you need is collected and that it is stored securely for only as long as it is needed.
- Data protection by design – you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.
- You should designate someone to take responsibility for data protection compliance within the LOC.

LOCs should use the useful self-assessment tool on the ICO website which takes you through each of these areas and provides full guidance https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr.

Table 1 - Individual Rights

There are the eight rights that individuals will have under the new GDPR

Rights	Details
The right to be informed	○ You must provide individuals with information about the data processing that is being carried out – this is usually provided in a Privacy Notice or Privacy Statement. ○ The information must be concise, transparent, intelligible and easily accessible, written in clear and plain language and free of charge.
The right of access	○ Individuals have the right to obtain confirmation their data is being processed and way and copies of that data. ○ More information on Subject access requests and timescales can be found on the ICO website https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/
The right to rectification	○ Individuals can have their personal data rectified if it is inaccurate or incomplete. ○ You must comply with any requests within one month of receipt. This can be extended to 2 months where the request is complex.
The right to erasure / be forgotten	○ Individuals have the right for their data to be erased. ○ This applies where the personal data is no longer necessary in relation to the purpose for which it was collected / processed. However, this does not apply where there is a duty to keep records for legal purposes eg. employment records. ○ If you have disclosed the personal data to third parties then you must inform them about the erasure of the personal data.
The right to restrict processing	○ Individuals have the right to 'block' or suppress processing of personal data. ○ When processing is restricted, you are permitted to store the personal data, but not further process it. ○ This is unlikely to apply in LOCs.
The right to data portability	○ This only applies when processing is carried out by automated means. This is unlikely to apply in LOCs.
The right to object	○ Individuals have the right to object to processing in some circumstances. ○ If *legitimate interests* was used as the lawful basis for processing personal data, you must stop processing data if an individual objects unless you can demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the individuals or the processing is for the establishment, exercise or defence of legal claims. ○ You must stop processing personal data for direct marketing if an individual objects.
The right not to be subject to automated decision-making including profiling	○ This is unlikely to apply in LOCs. ○ More information can be found on automated decision making on the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

Table 2 - Lawful bases for processing personal data

LOCs will need to have at least one lawful basis for processing personal data. This means having a legal basis for each processing activity.

Lawful bases for processing personal data	Details
Consent: the individual has given clear consent for you to process their personal data for a specific purpose	Should **NOT** be used as the lawful basis for health records or employee record. Most likely to be the lawful basis when data is processed for marketing purposes, only if *Legitimate interests* cannot be used. There are additional regulations to consider when using personal data for marketing, which can be found on the https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf
Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract	Likely to be used where data is held on LOC officers that is consistent with the contract of employment.
Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations)	Might be used by an LOC if needed to comply with a legal obligation.
Vital interests: the processing is necessary to protect someone's life	Less likely for LOCs to rely on this category.
Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law	Less likely for LOCs to rely on this category
Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)	Likely to be the lawful basis for most personal data held by LOCs. Health records cannot be processed on this lawful basis as they are also a special category of data (see below).

There are additional requirements for anybody processing special category data. This is defined as information about and individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life and sexual orientation. See the https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ for the conditions on processing special category data and the safeguards being put in place.

Note: You must determine your lawful basis before starting to process personal data. It's important to get this right first time. If you find at a later date that your chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.