General Data Protection Regulation (GDPR) for Primary Eyecare Companies

LOC SUPPORT UNIT
SUPPORT FOR PRIMARY EYE CARE DEVELOPMENT

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 Primary Eyecare Companies (PECs) to help them understand the changes and actions that they need to take and follows earlier guidance sent to LOCs.

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.

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.

Key Steps

Understanding the information you need to hold, what is personal identifiable information, where you store it and how you use it is key. PECs 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.

1. Awareness

It is important to ensure that decision makers and key members within the company are aware that the law is changing to the GDPR. They need to be aware the impact that this will have. This GDPR guidance should be read by all the directors, particularly those responsible for operational tasks that involve processing personal data, to include:

- Operational Lead
- Finance Lead
- Governance Lead

The new law increases the emphasis on organisations to demonstrate compliance and accountability in the handling and storage of personal data.

The ICO has clarified that 'You are expected to put into place comprehensive but proportionate governance measures.'

Rules around how data is stored haven't changed but it's useful to have a reminder:

- Any electronically held data should be in a password-protected secure environment and those passwords should be changed regularly and when access permissions change (e.g. someone steps down from the committee). Software should be up to date and anti-virus software installed.
- It can be easy to focus on digital/electronic data for GDPR but physically held data should be kept locked and secure too. Keys should be kept track of and combination codes changed regularly, and when access permissions change (e.g. someone steps down from the committee)
- Under GDPR how your data is stored by third parties is something you need to consider. It is your responsibility to ensure they are compliant with GDPR. This might be cloud or email services such as Google docs or Mail Chimp. Generally, the bigger more well-known organisations will have bases in the EU and will be GDPR compliant.

2. PECs should document all the personal data held

The record should include:

- PEC name and contact details
- a list of all the categories of personal data you hold - e.g. PEC board member records, PEC member records etc. The list should include all personal data held in both paper and electronic formats. Remember you only have to do this for personal data
- the legal basis on which you process personal data – changes in the law mean that it will be important to understand (and be able to explain) the legal basis you use to process personal data. Record the legal basis for holding each category of personal data – see Table A for a full list of the legal bases available
- where possible, include the time limits for erasure of the different categories of personal data
- where possible, include a general description of your technical and security measures – e.g. how you ensure ongoing confidentiality, integrity, availability and resilience of systems and services; how you would restore personal data in a timely manner in the event of a physical or technical incident; whether and now you test, assess and evaluate the effectiveness of technical and organisational security measures.

The Information Commissioners Officer has produced a sample document, and there is an example tab for PECs. This is documented in the attached spreadsheet and there is associated guidance here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/

2.1 Lawful bases for processing personal data

A lawful basis should be identified for any personal data that you process. This should be documented and also detailed in your privacy notice (see section 3).

The GDPR specifies lawful bases and a full list with examples is listed in table A, as identifying the correct lawful basis can be difficult. Legitimate interest is likely to be the lawful basis for most personal data held by the PECs.

There are three elements to the legitimate interests' basis. It helps to think of this as a three-part test. You need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

This can form part of a legitimate interests assessment (LIA) and a record should be kept, to ensure that you can justify our decision. More information can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

To support the first principle of GDPR, lawful and transparent processing, you may wish to send an update to inform constituents as to their new rights under GDPR and explain that the organisation intends to rely on Legitimate Interests as the lawful basis for communications. This is not mandatory under the Legitimate Interest definition of processing data sets but would constitute good practice. A summary of the legitimate interests' decision could be included in the update whilst the PECs online Privacy Policy should be sign-posted and is clear as to the constituent's right to object to further processing.

2.2 Consent

The lawful basis depends on the personal data held and also how you use it. There may be some cases where consent will be used as the lawful basis such as if a PEC engages in marketing. In these cases there is detailed guidance on how to manage consent and the ICO has published specific guidance and a checklist to review your practices https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in as consent cannot be inferred from silence, pre-ticked boxes or inactivity.
Consent must be separated from other terms and conditions and there must be simple ways for people to withdraw their consent.

If you are relying on consent to process data, ensure that it meets the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent and seek fresh GDPR-compliant consent or find an alternative lawful basis. Generally PECs will not be relying on consent however.

3. Privacy notices

Privacy notices contain information that should be available to individuals at the point at which you are collecting their data. They should be reviewed and updated if necessary, so they comply with the new rules. The GDPR states that privacy notices should be:

- concise and transparent
- easy to understand and access
- free of charge

The information that should be included differs depending on how you collected the information, but a summary is:

- who the data controller is
- purpose of the processing and the lawful basis for processing
- whether it will be shared with a third party and why
- the existence of each of the subject's rights
- the right to lodge a complaint with a supervisory authority.

You may need multiple privacy notices for different people/situations eg. one for PEC board directors, one for PEC constituents and one for people signing up to an email marketing list.

LOCSU is finalising a separate Data Policy and Privacy Policy which PECs may wish to use as template. This will be available on LOCSU's website from 25th May.

4. Requests from individuals

The GDPR includes the following rights for individuals, detailed in Table B, most of which are the same as those under the Data Protection Act but with some significant enhancements:

- 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
- the right not to be subject to automated decision-making including profiling.

PECs should check their procedures and consider whether any changes need to be made. For example, what would the process be if someone asks to have their personal data deleted: would your systems help you locate and delete the data? Who will make the decisions about deletion?

4.1 Subject access requests

The current DPA allows individuals to access personal data that is held about them in any format (subject to some safeguards). This will continue under the GDPR with two changes which will apply from 25 May 2018

- you will have a month to comply, rather than the current 40 days
- you will no longer be able to charge for complying with the request, unless a request is manifestly unfounded or excessive, e.g. for multiple further copies of the same information. Even then, you cannot charge more than the administrative cost of providing the information.

All PECs should review their subject access request procedure and plan how to manage them under the new rules.

5. Data Breaches

The GDPR has introduced a duty for all organisations to report certain types of data breaches to the ICO and in some cases to individuals.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

5.1 If a breach happens

When a personal data breach has occurred, you should establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay. The ICO has a dedicated personal data breach helpline https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

5.2 Data Processors

If you use a processor (see section 6.1), the requirements on breach reporting should be detailed in the contract between you and your processor. If this processor suffers a breach, then it must inform you without undue delay as soon as it becomes aware. You in turn notify the ICO.

For more details about contracts, please see the ICO draft GDPR guidance on contracts and liabilities between controllers and processors. https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

6. Roles and responsibilities

6.1 Data Controllers and Processors

The definitions of a **data controller** and **data processor** are likely to remain the same as under the existing law.

Data controllers – usually the PEC who has overall control and responsibility for how personal data is collected, processed and stored. The data controller is:

- responsible for determining how and why personal data is processed
- responsible (and liable) for personal data and any breaches
- responsible for reporting serious breaches to the ICO - with new reporting requirements (see section 5)
- ensuring that data processors – people and organisations who handle data on the data controller's behalf - comply with the law.

Data processors are all other persons who process personal data on behalf of the controller (other than a person who is an employee of the controller) e.g. external consulting companies. PECs may also be considered as data processors as well as data controllers. This will form part of discussions with commissioners when services are being contracted.

Data controllers and processes must have a contract in place which explains how obligations under the new data protection law will be managed. If you use a data processor you must be satisfied that they are fully familiar and compliant with GDPR. This is important as under the new rules, data processors will also become liable for breaches.

The ICO has published guidance and a checklist for contracts and would recommend PECs who use external processors to use this – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

6.2 Data Protection Officers and Data Protection Impact Assessments
Some, **but not all,** data controllers will have to appoint a Data Protection Officer (DPO) and/or perform a Data Protection Impact Assessment (DPIA).

PECs technically do not need to appoint a DPO or carry out a DPIA unless they carry out large-scale processing of special categories of data (see Table A).

However, we advise that it would be good practice to appoint a DPO. Commissioners are likely to expect a DPO will be in place. At the time of publication, we are aware that commissioners are already requiring DPOs for some PECs. The new NHS Standard Contract states that providers need to appoint a DPO where legislation requires. Legislation technically requires DPOs for GOS only; however, the likelihood is that commissioners are unlikely to draw distinctions between GOS and extended primary care services (such as MECs) in this context. This is particularly the case given the decision of Parliament last week to insist upon mandatory DPOs for GOS providers. As subcontractors to PECs will all be GOS providers, subcontractors will now need to have their own DPOs in place for their GOS work. In our view it will not be credible for PECs to argue against DPOs when their own subcontractors have these in place.

There is the further reality that competitors to PECs will have DPOs in place. Given the focus on governance made by commissioners, in our view it will not be credible for PECs to argue against DPOs being in place.

Points to consider before appointing a DPO or giving the title of DPO to a member of staff:

- the definition and scope of a DPO is very different under the new law. The DPO must have specialist knowledge of data protection law and work under conditions and terms specified in the new law
- PECs are strongly advised **not** to give the DPO title to a member of staff simply because they lead on data protection for the organisation
- if an existing staff member has the title of DPO, but your organisation is not required to have a DPO under the new law, then consider changing their title – e.g. to a Data Protection Lead or Data Protection Manager.

For more information contact:
Lisa Stonham: lisastonham@locsu.co.uk
ICO Website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Table A - Lawful bases for processing personal data

PECs 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 PEC board directors, staff 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 a PEC if needed to comply with a legal obligation.
Vital interests: the processing is necessary to protect the vital interests of a data subject or another person, where the data subject is incapable of giving consent	Less likely for PECs 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 PECs 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 PECs. 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; personal data 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 shall be prohibited, unless it satisfies at least one of the following conditions:	
Explicit consent of the data subject, unless reliance on consent is prohibited by EU or member state law	Less likely for PECs to rely on this category.
Necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement	PECs might rely on this category.
N**ecessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent**	Less likely for PECs to rely on this category.

Lawful bases for processing personal data	Details
Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent	Less likely for PECs to rely on this category.
Data manifestly made public by the data subject	Less likely for PECs to rely on this category.
Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity	It is possible that health care records and other special categories of data might have to be shared in this context – e.g. the final Data Protection Act in the UK might clarify sharing of patient records with regulators.
Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures	Less likely for PECs to rely on this category.
Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional	PECs likely to rely on this category when processing health records.
Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices	Less likely for PECs to rely on this category.
Necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)	Less likely for PECs to rely on this category.

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.

Table B - 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 PECs.
The right to data portability	○ This only applies when processing is carried out by automated means. This is unlikely to apply in PECs.
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 PECs. ○ 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/