GDPR Advice for Members

General Data Protection Regulation (GDPR) Changes effective from 25th May 2018

ABDO has produced this advice to assist practices in complying with the new requirements under GDPR. Currently all practices will be registered with the Information Commissioners Office (ICO) and have protocols in place to abide by current Data Protection laws, therefore you should review these and build on them to be compliant from 25th May 2018.

ABDO, with the Optical Confederation, communicated to members in December 2017, has been negotiating with Westminster. The organisations requested that optical practices be exempt from appointing a Data Protection Officer (DPO). Unfortunately despite our best efforts this request was unsuccessful and all optical practices, now defined as Public Authorities under the new GDPR, will need to appoint a DPO.

You will find below what practices should consider when reviewing their position on GDPR and the ICO guidance on these points.

Small business owners who do not have existing staff who could potentially be the DPO, who may struggle financially to fulfil their GDPR obligations in employing a DPO, are encouraged to do as much possible to become compliant by reviewing:

- registration with the ICO – new fees apply,
- all records held. Appropriately dispose of those that should no longer be held in line with GOC guidance and ICO guidance,
- privacy and security policies,
- protocols on reporting a breach,
- protocols in responding to a request for information.

Some members of ABDO with one person practices are working with local colleagues to be the DPO for each other, which is reasonable if the individuals have a good knowledge and understanding of GDPR requirements to comply.

Please note that this is guidance and you should visit the ICO website for more detailed information and explanations. There is also an ICO helpline to provide advice for small businesses too.

ICO website: https://ico.org.uk Tel: 0303 123 1113

What's new and how does this affect optical practices?

All data processing should be lawful, transparent and fair. The new GDPR law puts in place more requirements for businesses to make uniform processes they will already have in place:

- to prevent a breach (practices should be able to demonstrate all processes and have a DPO to manage GDPR under new law);
- to comply with data requests (you have one month to respond and you cannot charge under the new law);
- and to report a breach (72 hours to report a breach under new law).

You should not hold any personal information or health records any longer than necessary.

You should continue to abide by the GOC standards in this situation and consider the ICO advice that patient records contain personal data and should not be kept longer than necessary:

- Adult patient records should be retained for 10 years, following the last contact with the patient.
- In the case of children under 18, who have not been seen since their 18th birthday, you should keep records until their 25th birthday.
- For deceased patients, records should be kept for 10 years following the last contact with the patient.

What you need to review

Practices need to review processes considering the new rules on:

Individuals Rights

The ICO website has detailed guidance on all rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

You should continue to practice as you do currently with regards to providing GOS. This includes referring patients to secondary care, sending out reminders, appointments etc.

Communicating information/marketing on relevant products which are specific to your patients, which they currently expect, should remain the same too. Patients should always be given the option to opt out of receiving marketing material as they should be currently.

You should write to patients to inform them of your updated privacy policies, including your lawful basis under the new rules of GDPR.

Individuals have the right to access their record cards. This is known as a subject access request (SAR). Under the new rules you have one month to respond and you can no longer charge a fee for this. You should have a protocol in place for all SAR and make all staff aware of the process. Staff should also be made aware of the new law under GDPR including your practice process if there were a breach. Examples of SARs, Legitimate interests assessment (LIA), and privacy policy templates are available on the ICO website and the OC will be issuing further supporting materials soon.

Lawful Basis

Optical practices that provide General Ophthalmic Services (GOS) lawful basis is Public Task (You can use the interactive toolkit on the ICO website to confirm your lawful basis) and for all other processing within practices the lawful basis is a Legitimate Interest. All Practices Privacy notices should be reviewed to include your lawful basis and inform patients of this.

Public task - You can rely on this lawful basis if you need to process personal data:

- 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
- to perform a specific task in the public interest that is set out in law.

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.

The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.

Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

Legitimate interest is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.

It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

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.

The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required. See the ICO website for templates.

Data Protection Officers

Due to optical practices falling under the definition of a public authority within GDPR, all practices are required to appoint a DPO. A DPO cannot be the practice owner or someone that has financial responsibility within the practice. You should contact the ICO helpline if you fall under this category for them to advise you on exactly what you need to do to be compliant. A DPO can be an existing member of staff. You could share a DPO with other companies. There are also external companies that offer DPO services.

ABDO is working with the Optical Confederation on the role and requirements of a DPO in small practices to be accepted by the ICO and will communicate on this separately. We understand that for some practices that it may not be financially viable to appoint a DPO and if you need further advice, please email dmcgill@abdolondon.org.uk or contact the ICO direct on the number provided above.

The ICO guidance on a DPO is noted below:

What professional qualities should the DPO have?

The GDPR says that you should appoint a DPO on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law.

It doesn't specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires.

So, where the processing of personal data is particularly complex or risky, the knowledge and abilities of the DPO should be correspondingly advanced enough to provide effective oversight.

It would be an advantage for your DPO to also have a good knowledge of your industry or sector, as well as your data protection needs and processing activities.

The DPO's tasks are:

- to inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data processing
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

It is important to remember that the DPO's tasks cover all personal data processing activities.

When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.

The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.

If you decide not to follow the advice given by your DPO, you should document your reasons to help demonstrate your accountability.

The GDPR says that you can assign further tasks and duties, so long as they don't result in a conflict of interests with the DPO's primary tasks.

Please also note that there is no ICO recognised qualification/certificate for a DPO. There are companies that offer GDPR training but everything you need to know is on the ICO website.

Summary of Next Steps

You now need to:

- Review detailed guidance from the ICO
- Appoint a DPO
- Update Privacy Policies to include the lawful basis and communicate this to patients
- Implement protocols to comply with subject access requests (SAR)
- Carry out a legitimate interest assessment (LIA)

- Conduct a review of all record cards you hold and destroy those you are no longer required to keep by law
- Make all staff aware of new practice processes under the new GDPR requirements

The Optical Confederation will be issuing further detailed guidance which we will communicate in due course. In the meantime if you need further advice please email ABDO Policy Officer Debbie McGill dmcgill@abdolondon.org.uk