HUMBERSIDE LMCs

The professional voice of general practice

Appointing a Data Protection Officer (DPO) under the General Data Protection Regulation (GDPR)

Practice Management

HUMBERSIDE LMCs
The professional voice of general practice

Practice Management

Appointing a Data Protection Officer under the GDPR

The LMC is expecting to receive a high number of queries from practices in relation to the appointment of a Data Protection Officer (DPO) as part of the implementation of the General Data Protection Regulation (GDPR) in May 2018. There is a huge amount of information and guidance available relating to GDPR but much of it is difficult to navigate and some of it appears to give conflicting advice. In light of this, the LMC felt that it would be helpful to issue this information specifically in relation to DPOs, as this is an area where every practice will need to reach a decision about how best to proceed.

Do Practices have to appoint a Data Protection Officer (DPO)?

If you are a practice providing services under an NHS contract (and therefore a 'public authority' as defined in the Freedom of Information Act 2000), for the purposes of the GDPR, you will be considered to be a 'public authority'. As a public authority, you **must** designate a DPO in order to comply with the GDPR.

A DPO will help your practice to operate within the law by advising and helping to monitor compliance. Therefore a DPO will play a key role in your practice's data protection governance structure and to help improve accountability.

Who should I appoint as the practice DPO?

There needs to be a named (individual) DPO, but in practice it is likely that they may seek specialist assistance from others (whether internally or externally) – for instance on IT security issues, or legal matters.

Who to appoint is a decision to be made by the practice. Unfortunately, it is also an area in which there is much confusion and ultimately, who you appoint will depend on a number of different factors which will be different for every practice, such as the size of the practice.

Ultimately your choice of DPO should take account of:

1. knowledge of and comprehensive understanding of your practice's business and the personal data it processes;
2. knowledge of and skills in GDPR and information governance issues more generally; and
3. the importance of accessibility of the DPO and an individual's availability to undertake the role of the DPO, which may be onerous.

In theory, the options are:

1. Employ a DPO or designate an existing employee (with the appropriate expertise) to take on the role;
2. Appoint a GP Partner as your DPO (the current BMA guidance suggests that in some circumstances this might be possible providing that the role is defined to avoid or properly manage any conflict of interests that may arise, and decisions are documented); or
3. Designate an 'external' DPO – this could be provided by another local organisation with the appropriate staff and expertise on a contractual basis.

Appointing a Data Protection Officer under the GDPR

Any practice with doubts or concerns about making their DPO appointment should seek professional advice from a solicitor or an expert in data protection to ensure that you will be meeting the requirements of the GDPR in terms of the approach that is ultimately determined. This is because:

- You must be able to demonstrate that the DPO has the requisite knowledge and expertise which includes detailed knowledge of UK and EU data protection legislation and practices.
- You must ensure that the DPO is well resourced to be able to perform their tasks.
- You must be able to demonstrate that the DPO has an appropriate degree of independence within the practice and ensure that the DPO reports directly to your highest level of management.
- The DPO should not be expected to manage competing objectives that could result in data protection taking a secondary role to business interests. You must be able to demonstrate that the DPO does not determine the purposes or means of processing data within your practice. The GDPR stipulates that the data controller, namely a practice should ensure that tasks and duties of the DPO do not result in a conflict of interest. So, for example, anyone who is responsible for authorising or commissioning IT or manual records management systems (such as a particular GP partner or the Practice Manager) could be at risk of having conflicting duties if they also undertake the role of DPO. When considering possible candidates for the DPO role the practice should undertake a risk assessment to review the current duties of the proposed DPO in order to identify and then remove any potential conflicts of interest. This may mean reallocating some existing duties or placing additional safeguards in place for those duties such as making decision-making subject to the sign off of an additional person.
- You must ensure that the DPO does not receive any instruction regarding the exercise of his/her tasks and is protected from disciplinary action, dismissal or other penalties.
- You must ensure that the DPO is easily accessible as a point of contact for employees, individuals and the ICO.
- You must ensure that the contact details of DPO are published and communicated to the ICO.

If considering the appointment of an external DPO, practices may wish to explore a shared DPO. The current guidance is that DPOs may be shared by multiple organisations provided there is no conflict of interest. This would ensure consistency of approach and potentially an economy of scale. If progressing this approach, practices proposing to use the same DPO could jointly seek legal advice on any service contract to ensure that it is fit for purpose.

What does a Data Protection Officer do?

The Information Governance Alliance has produced helpful guidance on the role of the data protection officer in the health context which is available here:

https://digital.nhs.uk/media/35501/IGA-Guidance-on-the-GDPR-DPO-V1-FINAL/pdf/IGA_-_Guidance_on_the_GDPR_DPO_V1_FINAL

Appointing a Data Protection Officer under the GDPR

This includes a list at page 8 of the key components of a DPO's role mapped to the relevant Articles of the GDPR. This will provide useful guidance when writing a DPO job description or agreeing a contract/service level agreement with another organisation or person to provide this service to your practice.

Essentially DPOs help your practice demonstrate and assure compliance and are part of the enhanced focus on accountability within the legislation.

Do practices have to bear the costs associated with the appointment of a DPO?

Unfortunately, yes. There is no additional national funding to support practices with compliance and meeting the requirements of the GDPR. The LMC has approached our local CCGs to ascertain whether any local funding or other support can be made available to practices but have yet to receive a formal response.

LMC April 2017

HUMBERSIDE LMCs

The professional voice of general practice

The Humberside Group of Local Medical Committees Ltd

Albion House
Albion Lane
Willerby
Hull
HU10 6TS

01482 655111
humberside.lmcgroup@nhs.net
www.humbersidelmc.org.uk

@HumbersideLMC. Follow us for news and updates.