Data Protection Officers and GP practices under GDPR

What is a Data Protection Officer (DPO)?

A DPO has formal responsibility for data protection compliance within an organisation. The appointment of a DPO under the EU General Data Protection Regulation (GDPR) is only mandatory in three situations: when the organisation is a public authority or body, or when the organisation's core activities consist of either:

1. Data processing operations that require regular and systematic monitoring of data subjects on a large scale; or
2. Large-scale processing of special categories of data (i.e. sensitive data such as health, religion, race, sexual orientation, etc.) and personal data relating to criminal convictions and offences.

How does this apply to GP practices and their status as independent contractors?

All practices which provide services commissioned through NHS England are public authorities, therefore it is mandatory that they designate under the regulation, but they do not necessarily have to employ or retain, a DPO. However the designation must have taken place by 25th May 2018.

What are the options for a GP practice to appoint a DPO?

Designation is a decision to be made by the practice. The DPO is expected to monitor compliance, however, responsibility for compliance remains with the data controller and data processor. Large practices and multi-practice groups are likely to have in-house DPOs, but smaller practices may prefer to designate external DPOs that could for instance be provided by a Clinical Commissioning Group, Business Services Organisation or local/regional health board.

There are several options regarding designation of a DPO:

a) Employ a new member of staff with specific knowledge, qualifications and experience.

b) Appoint somebody who already works in the practice with the necessary knowledge, qualifications and experience, or who has the ability to acquire the necessary skills with suitable training. This person can add the DPO's requirements to other responsibilities, for example maintaining records of processing activities. DPOs must not be the final decision-makers regarding data processing; for example, they cannot be the data controller and must avoid any conflicts of interest.

c) Share a DPO with one or more practices. A CCG may be able to help facilitate this, but is unlikely to be able to fund such a person.

Although a practice must appoint a DPO, there is no reason why they shouldn't be supported in the role by a more experienced person, such as an information governance lead in the CCG, federation or group of practices. CCGs and/or federations could then develop a local network to support those with a DPO role in the area.

What if I choose to share a DPO?

In deciding upon a shared DPO you will need to consider factors such as:

- the sizes of the practices
- the numbers of patients
- whether the DPO is genuinely going to be in a position to understand and advise each individual practice and monitor compliance.

Does every DPO need to be an expert in data protection law?
No, Clause 97 states that in relation to the DPO; "... a person with expert knowledge of data protection law and practices should assist the controller", it then continues in the same clause with "The necessary level of expert knowledge..." So GDPR accepts there will be different levels of "expert knowledge" needed according to the sort of processing being done, some will need more expert knowledge than others. It is recognised that they will not fully understand all the ramifications of the new legal requirements from 25 May, and they will need to keep up to date with any changes and clarifications (for example from the ICO) and understand how these changes impact the practice, as the law becomes embedded. Their knowledge can be added to through a network of practice DPOs supported by a lead with the necessary expertise in the CCG or GP Federation.

What is the role of a DPO in a GP practice?
The DPO is an essential role in facilitating 'accountability' and the practice's ability to demonstrate compliance with the GDPR. What this means on a day to day basis is the DPO reports directly to the highest management level in the practice, normally the senior partner or partners. They don't require line management, but must have access to the senior management team of the practice.

The practice must also ensure the DPO has sufficient resources to undertake the role, including financial and human resources. As noted above, the DPO will need to keep up to date with any changes and clarifications and they must be supported by the practice to do so.

More specifically, the DPO will ensure that information governance and related policies address:

- practice accountability
- DPO reporting arrangements
- timely involvement of the DPO in all data protection issues
- compliance assurance: privacy by design and default
- advising on where data protection impact assessment is required
- the DPO's role in incident management

The practice must ensure the DPO is not told how to carry out their function and does not face any disciplinary action, dismissal or other penalties for carrying out their tasks as a DPO.

They must also ensure that where the DPO performs another function within the practice, there is no conflict of interest and that the contact details of the DPO are published in the practice's transparency information for subjects and are communicated to the ICO.

The DPO must not hold a position that leads him or her to determine the purposes and the means of the processing of personal data – this requirement will vary depending on whether the DPO is an internal or external appointment. In most cases, the data controller will be the GP practice rather than an individual GP and internal practice decisions about data processing (i.e. the purpose and means of processing) will be subject to the governance arrangements of the practice partnership. This means it might be possible for GP partners to fulfil the role of DPO provided the role is defined to avoid conflict of interests and decisions are documented.

In summary, the principal tasks of the DPO in a GP practice, as determined by the GDPR are:

- to provide advice to the practice and its employees on compliance obligations
- to advise on when data protection impact assessments are required and to monitor their

performance
- to monitor compliance with the GDPR and practice policies, including staff awareness and provisions for training
- to co-operate with, and be the first point of contact for the Information Commissioner
- to be the first point of contact within the practice(s) for all data protection matters
- to be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the practice's privacy notice
- to take into account information risk when performing the above

What else do GP practices need to do to be compliant with the GDPR?

The regulations require practices to identify and record what personal data has been collected from job applicants and carried through the employment lifecycle. This will cover data kept on HR information systems, in personnel files (both electronic and paper), and data saved on hard drives and emails. There isn't a prescribed format for how this data is held and it can take a variety of different forms as long as it fulfils the purpose of helping the practice to determine:
What personal data is collected?
Where is personal data stored?
How is personal data processed?

The GDPR requires a detailed record to be kept of personal data-processing activities - a data map such as outlined above can serve this purpose if it contains the necessary information.

Article 6 of the General Data Protection Regulation (GDPR) states that processing of personal data will be lawful only if at least one of the following conditions applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the data controller is subject;
- Processing is necessary to protect the vital interests of the data subject or of another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (this condition does not apply to processing carried out by public authorities in the performance of their tasks).

Practices will need to look at the types of employee data they process and the processing activities they use and then determine which justification or justifications are relevant.

If it's not possible to justify the processing activity with one of the available grounds, the practice will have to stop processing.

Practices will have to take several technical and organisational measures to make sure data protection is incorporated into all procedures involving personal data. This will mean taking the following steps:

- Reviewing policies and processes to ensure that only necessary data is collected, and that it is only processed to the extent necessary;
- The data must be stored securely;
- Access to the data must be limited;
- The data must be destroyed once it's no longer needed.