Data Protection Officer (DPO): Top Tips and Advice

This guidance document – written as an appendix to Step1 of the Guidance for Community Pharmacy (Part 1) – brings together some top tips and formal advice for appointing a DPO.

Top Tips

A DPO:

- is an expert of GDPR and data protection but this means in the context and to the extent required for the individual position – for you as a contractor and in your community pharmacies (perhaps using the Community Pharmacy GDPR Working Party guidance and other information to become such an expert);
- is for the contractor and all its community pharmacies (it is not a different DPO for each pharmacy);
- may be the DPO for a number of contractors – or your GDPR person could be the DPO for another local contractor and its GDPR person could be your DPO;
- must be sufficiently senior or experienced to provide advice to the decision-makers in the community pharmacy;
- is named on the privacy notice and is the point of contact for patients and the Information Commissioner's Office (ICO) (potentially this makes an in-house DPO better);
- must have knowledge of the business and understand the data flows and the risks involved;
- is not operational – meaning he or she should not be the person who decides how the pharmacy runs/operates/acts as regards data flows;
- could be the superintendent pharmacist – but not if he or she makes all the decisions in the community pharmacy;
- may be an appropriately skilled pharmacy technician in appropriate circumstances, for example, for a contractor with one or two pharmacy premises;
- may also be the Information Governance (IG) Lead if the IG Lead only influences and implements policy on data flows and does not determine the purpose and means of processing of personal data (i.e. does not decide how the pharmacy runs/operates/acts with regard to data flows); and
- is generally NOT needed by an LPC (exceptionally a DPO may be needed, for example, if it processes personal data concerning health on a large-scale).

Should you appoint an internal or external DPO?

PSNC suggests an internal DPO if possible for his or her knowledge of the business and because knowledge of GDPR can be gained from Community Pharmacy GDPR Guidance and Workbook and getting to grips with GDPR articles etc AND because liability issues are contained in-house AND the contractor's point of contact is likely to be easier for patients to contact and be easily able to give a quick answer to a question or concern. An internal appointment is also likely to cost less than an external appointment, provided that the internal DPO can provide appropriate advice.

We have some guidance with our announcement at:
https://psnc.org.uk/our-news/gdpr-action-needed-appointing-a-data-protection-officer/

Formal Advice

Please note, the NPA is leading on this issue for NPA members. Non NPA members should consider the following advice from the NHS Digital's Information Governance Alliance (IGA).

We suggest you consider the advice provided by NHS Digital's IGA which includes the following:

4.1 The organisation's responsibilities – the position of the DPO

The DPO is an essential role in facilitating 'accountability' and the organisations ability to demonstrate compliance with the GDPR. The organisation must appoint a DPO whose job description is compliant with GDPR requirements and, in particular, must ensure:

- that the DPO role directly reports to the highest management level of the organisation – this does not necessarily imply line management at this level, but direct and unimpeded access to the senior management team
- that the DPO role is provided with adequate resources: financial and human resources, and is supported in maintaining his or her expertise
- that the DPO has proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the GDPR, and sufficient understanding of the organisation's business and processing
- that information governance and related policies address - organisational 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.
- that the DPO does not receive any instruction regarding the exercise of his or her tasks, and is protected from disciplinary action, dismissal or other penalties
- that where the DPO performs another role or roles, that there is no conflict of interest
- that the contact details of the DPO are published in the organisation's transparency information for subjects and are communicated to the ICO.

It is important to consider EU Guidelines that:

'[t]he DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case'

and further:

'As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing'

So, positions that involve the authorising or commissioning of IT or manual records management systems are likely to meet the criteria for determining the purposes and the means of processing.

DPOs may be shared by multiple organisations that are 'public authorities' taking into account organisational structure and size and may be either a member of staff or may fulfil the tasks on the basis of a service contract, provided there is no conflict of interest. A DPO team with a nominated contact for each organisation is an acceptable approach.

Also, that:

4.2 The qualities and tasks of the DPO

The DPO shall be designated on the basis of professional qualities and, in particular:

- expertise in national and European data protection laws and practices and an in depth understanding of the GDPR
- sufficient understanding of the processing operations carried out, as well as the information systems and data security and data protection needs of the organisation
- demonstrable ability to fulfil his or her tasks. The principal tasks of the DPO from the GDPR are:
- to provide advice to the organisation 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 organisational 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 organisation(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 organisation's privacy notice
- to take into account information risk when performing the above.

The full guidance is on NHS Digital's IGA website.