GDPR Advice Sheet:
Data Protection Officers

technologytamed
Computer Support & Services

Introduction

Many clinics are expressing concern or confusion regarding the need for a Data Protection Officer (DPO), so I am hoping this advice sheet may help to clarify matters.

Glen Mansbridge, March 2018

Disclaimer

Technology Tamed Limited is not legally qualified. Some of the regulations are open to interpretation and clarity for some aspects will only be obtained long after May 25th. In addition, some of the finer detail is still being clarified by the EU at the time this toolkit was written and as such may change the intention, meaning or interpretation of any part of the regulations.

If you need clarification on any aspect of GDPR you should seek specialist legal advice. Technology Tamed Limited, or its employees, cannot accept any liability for any loss or damage you may incur as a result of the material in this toolkit.

What the Regulation says:

Article 37 of GDPR states:

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

As health data constitutes special categories of data then this will be a requirement for some clinics.

What is “large scale”?

The regulation does not define large scale and neither does the ICO website. The European Parliament has requested an amendment to GDPR to quantify large scale:

“Finally, Parliament adds that a DPO should be mandatory for all enterprises that process 'Special categories' of data, including information such as health data or religious and political beliefs. The Commission text requires any enterprise over 250 employees, while the Parliament text calls for those processing the personal data of over 5000 data subjects in any 12-month period.”

There is no timescale for this change to be discussed, agreed or implemented.

GDPR Advice Sheet:
Data Protection Officers

technologytamed
Computer Support & Services

What the ICO says:

When I spoke to the ICO a few weeks ago I gave them some examples of clinics with specific number of patient records and asked whether they would expect a DPO to be appointed. In the cases of clinics having 20,000 records, the response was instantly "yes", as it was for 10,000 records and 5000 records. The ICO went on further to explain that it would be seen as good practice for all clinics to appoint a DPO, regardless of how many patients records you hold. I confirmed that the role of DPO should not be given to someone who is directly involved in processing the data (to avoid a conflict of interest) yet for most clinics, everyone employed is processing this data. Their response was that the clinic could always outsource this role to a third party.

This resulted in the advice given in stage 3 of the toolkit. Understandably this has caused some concern amongst you, especially those smaller clinics and sole practitioners. As a result, I have just completed an online chat with the ICO and here is the transcript of the conversation:

[9:01 AM] ico_jand:	Hello, have you had a look at our guidance on DPO?
[9:02 AM] glen mansbridge:	Yes I have. I am a sole chiropractor with approx. 1000 patient records, of which only a fraction are active, the remaining are being kept for the statutory 8 years. Do I need to appoint a DPO?
[9:04 AM] ico_jand:	That's a decision for you to make. As an independent regulator we can't make these de cisions for you. If you have read the guidance and e.g. you are of the opinion that you don't need a DPO then document that assessment and keep on record.
[9:05 AM] glen mansbridge:	The regulation states that if I am processing large scale of special categories of personal data I MUST appoint a DPO. At what point would the ICO consider my business as being large scale? 5000 records? 10000 records? 20000 records?
[9:05 AM] ico_jand has joined the room	
[9:09 AM] ico_jand:	We don't have a measurement as such so I wouldn't be able to tell you. We are new to the concept too.
[9:10 AM] glen mansbridge:	Part of the remit of the ICO is to enforce the regulations yet effectively as you cannot state what this measurement is, then it is unenforceable until there has been case law and precedents. Is that a fair assessment?
[9:12 AM] ico_jand:	Yes.
[9:13 AM] glen mansbridge:	This is what I expected but is contradictory to the advice I was given a few weeks ago when I rang the ICO regarding this same matter. Then I was told definitively that clinics with even 5000 records would need to appoint a DPO.
[9:15 AM] ico_jand:	There is no defined threshold, and the decision as to whether you have to appoint a DPO is yours to make.
[9:15 AM] ico_jand:	Defined as in 0/1.
[9:16 AM] glen mansbridge:	Thank you for your clarification in this matter.

[9:16 AM] ico_jand: If you were a public authority it is clear. But large scale unfortunately is not a 0/1.

[9:17 AM] glen mansbridge: Understood - thank you once again for your advice

[9:17 AM] ico_jand: Thank you for using our live chat service. Have a good day.

As a result of this online chat my view on this matter is that if you feel that appointing a DPO is appropriate for your clinic then do so, otherwise wait until case law or revisions to the regulation give us a usable definition of "large scale". I would recommend you keep a copy of this advice sheet in your GDPR Compliance manual to show that the role of DPO has been considered along with the transcript of the advice from the ICO.

What if you want to appoint a DPO?

- If you employ a practice manager who does not, as part of their role, directly input patient data then arguably there would be no conflict of interest so they could be the DPO. Note that they need to be proficient in GDPR as the responsibilities of a DPO include handling all matters relating to GDPR for the clinic, including procedures, data subject access requests, data protection impact assessments and data breaches.

- A family member (who does not process the data) may be a willing volunteer! As with the practice manager they have to be suitably knowledgeable about GDPR.

- Outsourcing may be an option for you. Various organisations are offering this service (including Technology Tamed) and this may be a cost-effective way to ensure you maintain compliance.

- Minimise your data. Rather than keep patient treatment notes "forever", destroy them after the minimum period. If you have not seen a patient for 8 years, you will need to take new history and give them a full examination, so not having their notes from, for example, 20 years ago may not be an issue. The less data you hold, the lower the risks and the need for a DPO may be less significant.

