LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Issues for public sector bodies appointing a Data Protection Officer under the GDPR

by **lk-shields**

Issues for public sector bodies appointing a Data Protection Officer under the GDPR

6th January 2017 | by

The General Data Protection Regulation (GDPR) was adopted into EU law this year. It will come into force in Ireland on 25 May 2018.

The GDPR is a significant overhaul of data privacy law in the EU. In the intervening period it is necessary for organisations to plan how they will meet their obligations under the GDPR.

A significant change, introduced by Article 37 of the GDPR, is that all public authorities and bodies (except for courts) must appoint a Data Protection Officer (DPO).

A new role with legal status

Some public bodies already have a person designated to deal with data protection issues, such as access requests under the Data Protection Acts 1988 and 2003. However the GDPR constitutes a new role of DPO which must conform to specified rights and responsibilities. The GDPR places specific obligations on a DPO and grants the person considerable autonomy in the exercise of the role. The DPO role requires planning and the allocation of resources to ensure compliance with the GDPR principles of transparency and accountability. Employing a person in this new role will need proper appraisal before May 2018, when the person must be in situ.

Who should be appointed as a DPO?

The GDPR provides that a DPO may be either an employee or engaged under a service contract. The DPO must be appointed on the basis of professional qualities, in particular "expert knowledge of data protection law and practices". DPOs do not have to be lawyers, but it is probable they will have a legal or specialist qualifications and training in data protection law to satisfy this test. A DPO will need to have a good understanding of a body's technical and organisational structure and its technology infrastructure.

Corporate Governance

The GDPR provides that the DPO must report directly to the “highest management level of the controller or the processor". This means that a DPO will need to have a direct reporting line to the most senior level in the public body, whether it is the Secretary General of a Department or the equivalent. Public bodies will need to be able to demonstrate that such reporting lines exist, are transparent and do not compromise the DPO's independence.

Ensuring the independence and integrity of the DPO

From the outset it will be important for each public body to demarcate the role of its DPO within its organisation's structure. The GDPR requires the DPO's responsibilities to include:

- Advising on and developing the body's data protection policies and procedures;
- Monitoring implementation of procedures and ensuring they are transparent and accessible;
- Communicating with the Data Protection Commissioner on behalf of the organisation; and
- Engaging with individuals internally and externally on data privacy issues.

Selecting the right candidate will be a serious matter for any organisation appointing a DPO. An organisation is prohibited by the GDPR from instructing a DPO about how he or she exercises the role. A DPO cannot be dismissed or penalised by the controller or the processor for performing his or her tasks. This means that an employee's performance as DPO cannot be managed in the normal way. To avoid uncertainty about employment relations some public bodies may instead elect to appoint outside contractors as DPOs.

A DPO must be involved in all organisational areas dealing with data protection. Public bodies are obliged by the GDPR to provide DPOs with the resources necessary to execute their tasks and to maintain their expert knowledge. Therefore great care will be required when establishing structures to protect a DPO, which taking account of employment laws and the objectives and governance of the public body. In early 2017, public sector management should begin addressing how they will structure, procure, train and resource their DPOs to the standards set out in the GDPR.

For more information on this topic, please contact any member of our Intellectual Property, Technology and Privacy team at +353 1 661 0866.

This article first appeared in the Public Sector Times, December 2016.

About the Author