GDPR and the Role of the Data Protection Officer

The clock has started on the biggest change to the European data protection regime in 20 years. After four years of negotiation, the new EU General Data Protection Regulation (GDPR) will take effect on 25th May 2018.

In the UK, it will replace the Data Protection Act 1998 (DPA). With some GDPR breaches carrying fines of up to 4% of global annual turnover or 20 million Euros, now is the time to start planning (if you have not already started!).

You might be forgiven for thinking that the Brexit vote means that there is no need to worry about GDPR (being a piece of EU legislation) or that its effect will be time limited. The Government has now confirmed that GDPR is here to stay; well beyond the date when the UK finally leaves the European Union.

Section 4 of GDPR introduces a statutory position of Data Protection Officer (DPO) who will have a key role in ensuring compliance with GDPR. But who exactly will need a DPO and what is his/her role? The Article 29 Data Protection Working Party has now clarified this in its recently published guidance (the A29 Guidance) and a useful FAQ. Technically these documents are still in draft as comments have been invited until the end of January 2017.

Who needs a DPO?

For the first time Data Controllers as well as Data Processors are required to appoint a Data Protection Officer in three situations (Article 37(1)):

a) where the processing is carried out by a public authority or body

Public authorities and bodies are not defined within the legislation. The guidance says that this is a matter for national law. It's fair to say that all bodies subject to the Freedom of Information Act or the Freedom of Information (Scotland) Act will be covered by this requirement e.g. councils, government departments, the health sector, schools, emergency services etc. However it is likely to also cover private companies that carry out public functions or deliver public services in the area of water, transport, energy, housing etc. (See also the decision in Fish Legal v Information Commissioner and others [2015] UKUT 0052 (AAC) which considers the definition of public authorities under the Environmental Information Regulations 2004.)

Purely private companies not involved in public functions or delivering services will only need to appoint DPO if they engage in certain types of data processing operations explained in Article 37:

> ***b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale***

Under this provision companies whose primary activities involve processing personal data on a large scale for the purposes behavioural advertising, online tracking, fraud prevention, detection of money laundering, administering loyalty programs, running CCTV systems, monitoring smart meters etc. will be caught by the DPO requirement.

> ***c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences***

The A29 Guidance states that the "and" above should be read to say "or" (a diplomatic way of saying the proof-readers did not do their job!). Special categories of data are broadly the same as Sensitive Personal Data under the Data Protection Act 1998 e.g. ethnic origin, political opinions, religious beliefs, health data etc. This provision will cover, amongst others, polling companies, trade unions and cloud providers storing patient records.

Unless it is obvious, organisations that don't need to appoint a DPO should keep records of their decision making process. The A29 Guidance suggests that it will be still be good practice to appoint a DPO in some cases; for example, where private organisations carry out public tasks. This could include companies delivering core public services under an outsourcing arrangement e.g. housing maintenance companies, charities delivering social services etc. A group of undertakings may appoint a single DPO provided that he/she is easily accessible and there are no conflicts of interests.

Even organisations not based in the EU may be caught by GDPR and the requirement to appoint a DPO. GDPR will apply to any entity offering goods or services (regardless of payment being taken) and any entity monitoring the behaviours of citizens residing within the EU. Companies are now directly responsible for DP compliance wherever they are based (and not just their EU based offices) as long as they are processing EU citizens' personal data.

The DPO's Tasks

According to Article 37(5), the DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness- raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO in the UK);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data

Qualities

The A29 Guidance states:

> *"Although Article 37 does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs should have expertise in national and European data protection laws and practices and an in depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs."*

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a

large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. The necessary skills and expertise include:

- expertise in national and European data protection laws and practices including an in depth
- understanding of the GDPR
- understanding of the processing operations carried out
- understanding of information technologies and data security
- knowledge of the business sector and the organisation
- ability to promote a data protection culture within the organisation

Act Now has recently launched its GDPR Practitioner Certificate aimed at up skilling existing and future DPOs in both the public and private sector. To learn more please visit our website www.actnow.org.uk.

The DPO must be allowed to perform tasks in an independent manner and should not receive any instructions regarding the exercise of their tasks. He/She reports to the highest management level in the organisation and cannot be dismissed or penalised for doing their job.

Resource Implications

Article 38(2) of GDPR requires the organisation to support its DPO by "providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge." The A29 Guidance says that, depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- Active support of the DPO's function by senior management
- Sufficient time to for DPOs to fulfil their duties
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- Official communication of the designation of the DPO to all staff
- Access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- Continuous training

The DPO will be at the heart of the data protection framework for many organisations, facilitating compliance with the provisions of the GDPR. Now is the time to appoint one to ensure that you get the most suitably qualified. Some say 28,000 will be required in the UK and US. Others have even suggested there will be a skills shortage!

There is certainly a lot to learn and do in less than 18 months when GDPR comes into force. Training and awareness at all levels needs to start now.

Make 2017 the year you get prepared for the General Data Protection Regulation (GDPR). See our full day workshops and new GDPR Practitioner Certificate.