GDPR in Context: Data Protection Officers

Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

Overview

A significant new obligation under the GDPR is the requirement for certain types of companies, whether acting as controllers or processors, to appoint a data protection officer ("**DPO**"). While DPOs are not a new concept, the GDPR is the first EU wide legislation to mandate DPOs in some circumstances, and to describe the role in detail.

The need for a DPO

In particular, the requirement to appoint a DPO will apply to:

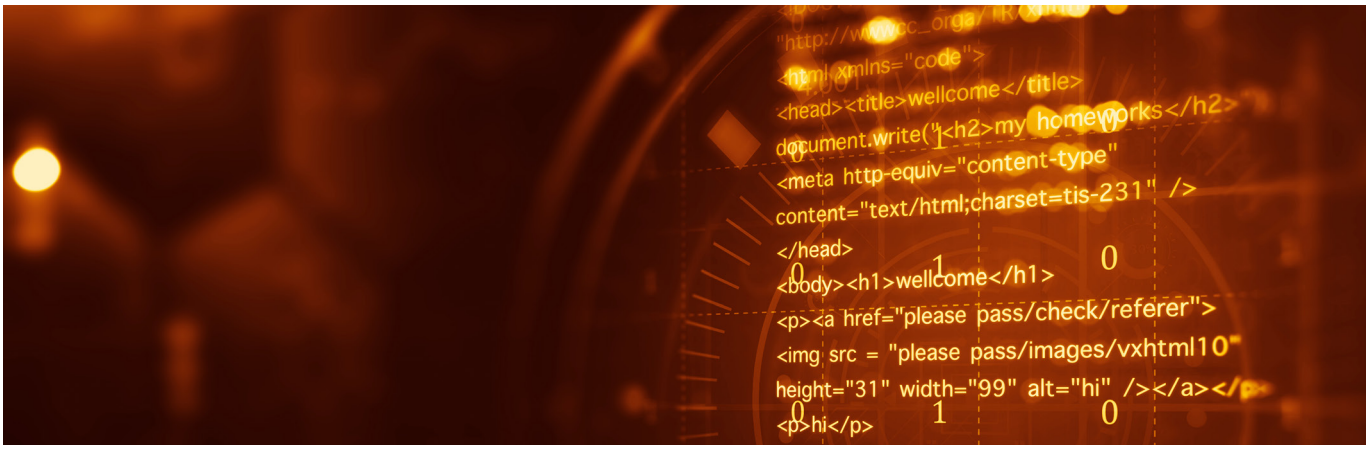
- companies whose core activities consist of:
- data processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale; or
- processing on a large scale of the special categories of data and data relating to criminal convictions; and
- all public bodies and authorities (other than courts acting in their judicial capacity).

In addition, EU member states may specify other circumstances in which the appointment of a DPO will be mandatory within that EU member state.

The Article 29 Working Party ("**WP29**"), in one of its earliest commentaries on the detailed provisions of the GDPR, published guidance on DPOs and has recommended that, unless it is obvious that an organisation is not required to designate a DPO, the internal analysis carried out to determine whether or not a DPO is to be appointed be documented, in order to demonstrate that the relevant factors have been properly considered.

In that regard, the "*core activities*" of an organisation should be viewed as those key operations necessary to achieve the organisation's goals (including activities which are an inextricable part of the organisation's activities). In assessing whether a processing activity is carried out on a "large scale", a number of factors, including the number of data subjects concerned, the volume and / or the range of data, the duration or permanence of the processing, and the geographical extent of the processing, will all be relevant considerations.

The WP29 sets out a number of examples of large scale processing, including processing of customer data in the regular course of business by an insurance company or a bank, behavioural advertising by a search engine, and data (content, traffic, location) processing by telephone or internet service providers. The WP29 also points out that "*regular and systematic monitoring*" is not restricted to online behaviour and monitoring, and gives examples of profiling and scoring for credit scoring, fraud or anti-money laundering prevention purposes, location tracking, and fitness and health tracking by wearable devices, as examples of the types of monitoring which, if large scale, will trigger an obligation to appoint a DPO.

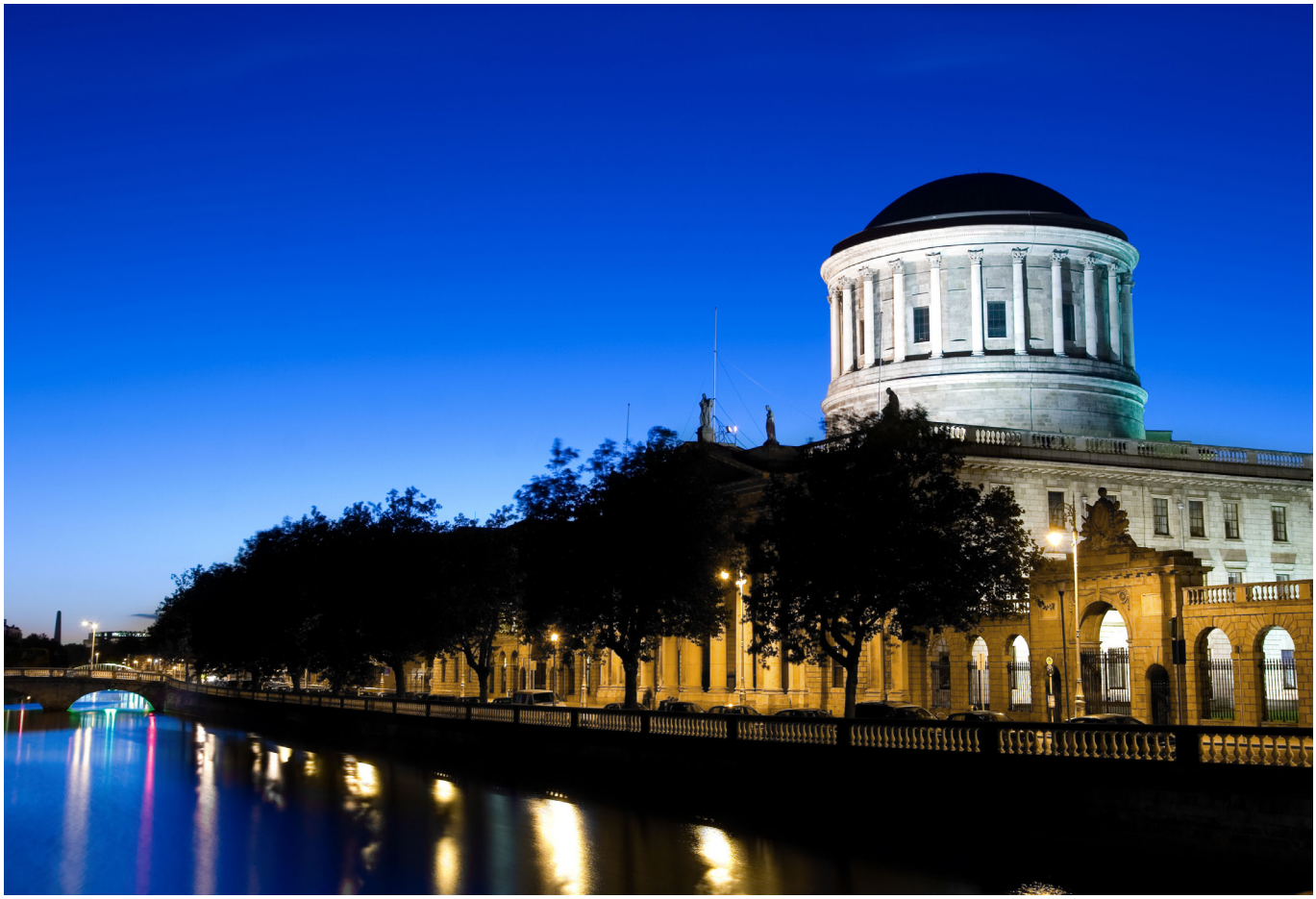


[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Data Protection Officers

Opting for a DPO

Other companies may opt to appoint a DPO, but where they choose to do so, will be subject to all DPO related provisions in the GDPR. Provided that there is no confusion regarding title, status, position and tasks, this will not prevent such organisations appointing staff or consultants to undertake data protection related tasks, without those individuals being DPOs. However, this distinction needs to be made clear in all internal and external communications.



Identifying the DPO

Filling the role of DPO cannot be a mere 'box ticking' exercise. The DPO must have expert knowledge of data protection law and practices, and other relevant professional qualities, and must be in a position to fulfil the tasks specified below. For many companies, this may require creating a new role and hiring a dedicated expert.

Some companies may not need a dedicated full-time DPO, and the GDPR does allow some flexibility on this. A DPO may be part time, and an existing employee can serve as the DPO, provided they have the required expertise and any other role they hold in the organisation does not give rise to a conflict of interests with the DPO role.

A group of related companies can appoint a single DPO provided that the DPO is easily accessible from each relevant establishment. The WP29 has described accessibility in terms of DPO availability to communicate efficiently with data subjects, supervisory authorities and internally within an organisation, whether that means the DPO is present physically on the same premises or via a hotline or other secure means of communication.

Alternatively, an external DPO can be appointed under an appropriate service contract, although in this case the appointing organisation would need to be comfortable that the external DPO has sufficient understanding and knowledge of the particular processing operations, information systems, data security and data protection needs of the organisation, to be able to discharge his / her functions. It is also possible for associations of processors or controllers to appoint a DPO to represent the association.

Details of the DPO must be published by the relevant organisation, and must also be notified to the relevant supervisory authority (notwithstanding that registration requirements for controllers and processors will generally fall away following GDPR coming into full effect). Data subjects must also be permitted to contact the DPO directly in relation to processing of their data and exercise of their rights.

Data Protection Officers

The role of the DPO

The DPO will be required to have due regard to the risks associated with the processing operations, taking into account the nature, scope, content and purposes of the processing, in fulfilling his / her responsibilities, which emphasises that the DPO will need to understand the particular processing operations of the organisation(s) to which he / she is appointed. The GDPR makes clear that the role is an independent one, and DPOs cannot be "instructed" on the discharge of the DPO responsibilities or on any data protection matter or issue.

Those responsibilities include:

- informing and advising the company and its employees of their respective obligations under the GDPR and data protection legislation generally;
- monitoring compliance with the GDPR, data protection legislation and the organisation's own data protection policies. This will include assignment of responsibilities, awareness-raising and staff training, and related audits;
- providing advice on data protection impact assessments ("**PIAs**") (the GDPR separately obliges a controller undertaking a PIA to seek the advice of the DPO, where one has been designated); and
- acting as a point of contact for and cooperating with the organisation's supervisory authority.

A DPO is permitted to undertake other tasks, subject to there not being any conflicts of interest, and the WP29 has pointed out that an organisation may assign the DPO with the task of maintaining the record of processing operations which both controllers and processors are required to maintain under the GDPR.

The role and obligations of the organisation

The DPO will need to be involved, properly and in a timely manner, in any data protection-related issues affecting the organisation, including for example any breach issues and notifications. The organisation will be expected to provide the DPO with the resources (including time, staff and infrastructure) necessary to carry out his / her tasks and for him / her to maintain his / her expert knowledge on data protection matters, and will also need to provide the DPO with access to all personal data and data processing operations.

Data Protection Officers

Independence of the DPO

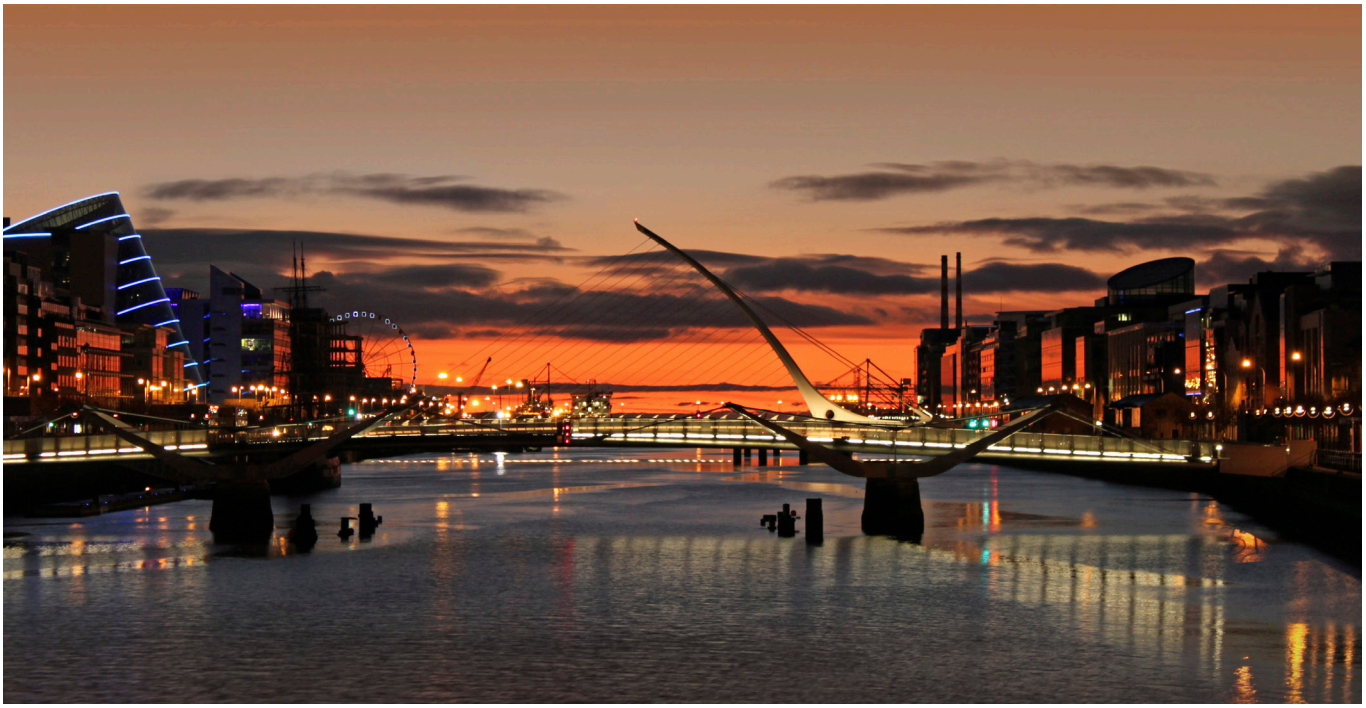
However, the organisation must also ensure that the DPO does not receive any instruction with regard to his / her tasks, and that the DPO's reporting line is to the highest level of management in the organisation. These requirements, and the express statement in GDPR to the effect that the DPO cannot be dismissed or penalised for fulfilling his / her tasks, thereby ensuring the necessary degree of autonomy and independence for the DPO, emphasise the importance which organisations will be expected to attach to data protection under GDPR, and in particular in those cases where a DPO appointment is mandatory. The WP29 recommends that due weight be given to the views of the DPO, who must be permitted to voice dissenting views in respect of an organisation's decisions, and that the reasons for any decisions not to follow the DPO's advice be documented.

Importantly, it is the relevant organisation, and not the DPO personally, which remains responsible for compliance with the GDPR, although appointment of and adherence to the guidance of a DPO may assist in demonstrating compliance with GDPR requirements.

Next steps

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning customer data and other personal data which it controls, and that it puts appropriate notifications, processing agreements, transfer arrangements and security arrangements in place.

It will be important that organisations whose activities might trigger the requirement for a DPO prepare themselves well in advance of the deadline. A properly qualified and resourced DPO should not, however, be viewed as a burden, but as a means of assisting an organisation in meeting the often complex data protection requirements under the GDPR and national laws, and ultimately in being able to demonstrate compliance with those obligations.



Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com