information commissioner
Barrantagh Fysseree

Article 29 Working Party has published the first formal GDPR Guidance

After its December Plenary meeting, the Article 29 Working Party (WP29), which will become the European Data Protection Board (EDPB), published its first GDPR guidance and FAQs providing interpretation in three areas:-

- **Data Protection Officers**
- **Lead Supervisory Authorities**
- **Data Portability.**

The following summarises the main points in that guidance , but controllers and processors that provide goods or services to EU residents or process personal data on behalf of an EU data controller should familiarise themselves with the entire guidance.

There is less than eighteen months until the GDPR becomes enforceable on 25 May 2018 and the guidance provides a first indication of the future expectations.

GDPR CONFERENCE
VILLA MARINA
10 May 2017

The Commissioner, in association with Isle of Man Government, is arranging a conference aimed at Directors, senior managers and compliance officers to explain the impact of the GDPR, it sanctions and penalties and the new regulatory environment at local, UK and European levels.

More information is available from the Commissioner's website at: GDPR Conference

If you would like to register your interest in attending forward your details to us at:

ask@inforights.im

Priority will be given to those that register an interest before 27 January 2017

DATA PROTECTION OFFICERS

Guidance:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

FAQs:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf

Articles 37 to 39, of the GDPR make provision for the designation, position and tasks of the Data Protection Officer (DPO). Accordingly the guidance is split into similar sections.

DPO DESIGNATION

Under Article 37(1) a DPO is required when:-

> a) the processing is carried out by a public authority or body;
> b) 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; or
> c) 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 guidance provides an explanation of what is meant by core activities, regular and systematic monitoring and large scale processing which would require a data controller or data processor to appoint a DPO.

The guidance expects that a DPO will be designated by banks and insurance companies and by any controller or processor that undertakes processing for purposes including fraud prevention and anti-money laundering.

The WP29 emphasises its view that as a matter of good practice all controllers and processors should consider appointing a DPO whether or not there is a requirement to do so, but stresses**:**

> *"Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly."*

External DPO

The guidance confirms that the functions of a DPO may be carried out by an individual or organisation outside the controller or processor's organisation on the basis of a service contract. However it is also stressed that accessibility to and availability of the DPO is essential.

Responsibly for compliance
While the DPO's main tasks will concern compliance with the GDPR, the guidance confirms that DPOs are not personally responsible for any non-compliance. That responsibility remains with the controller or processor and its directors, etc**.**

Expertise and Skills
The level of expertise required of a DPO must be commensurate with the sensitivity, complexity and amount of data an organisation processes. A DPO should have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR.

Knowledge of the business sector and of the organisation of the controller is also expected and the DPO should have a sufficient understanding of the processing operations carried out, including information systems, as well as the data security and data protection needs of the controller. *(See: Conflicts of Interest below.)*

In the case of a public authority or body, the DPO should have a sound knowledge of the administrative rules and procedures of the organisation.

Conflict of interests
Article 38(6) allows DPOs to 'fulfil other tasks and duties', however, it also states that '*any such tasks and duties do not result in a conflict of interests*'.

DPOs are expected to act in an independent manner and DPOs may undertake other duties, provided they do not give rise to conflicts of interests. In particular the 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.

Conflicting positions include senior management positions, such as CEO, COO, CFO, Head of HR or Head of IT.

Lead Supervisory Authorities

Guidance:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf

FAQs:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_annexii_en_40858.pdf

The guidance is not specifically directed at controllers or processors in third countries such as the Isle of Man but nonetheless it does explain what to consider in identifying the lead EU supervisory authority for its processing. Isle of Man based controllers or processors should find the guidance on "group of undertakings" and "substantially affects" helpful.

Data portability

Guidance:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

FAQs:
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf

Data portability is one of the new rights set out in the GDPR.

As explained in the FAQs, data portability provides the ability for data subjects to obtain and reuse "their" data for their own purposes and across different services. This right facilitates their ability to move copy or transfer personal data easily from one IT environment to another, without hindrance. In addition to providing consumer empowerment by preventing "lock-in", it is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner under the control of the data subject**.**

Get in touch

If you have questions about the GDPR, or would like to make comments about the content of any of our publications, please contact us.