
# GDPR conundrums: The data protection officer requirement

**Lokke Moerel**

**One for all ... Maybe?**

The General Data Protection Regulation introduces a general EU-wide obligation to appoint a data protection officer for controllers and processors involved in high-risk processing activities, i.e., where one of a company's core activities is the large-scale monitoring of individuals or processing of sensitive data. This obligation has been one of the most debated and amended provisions in the legislative process of the GDPR. It was also one of the reasons the German government opposed the GDPR taking the form of a regulation as this would set aside the current German requirement for nearly all controllers to appoint a DPO.

The proposals truly flip-flopped:

- *From* a mandatory requirement to appoint a DPO, which would override national requirements to appoint a DPO in the Member States even if those requirements are stricter (Commission's initial proposal),
- *… to* appointment of a DPO being fully voluntary (Council's version),
- *… and ultimately to* a mandatory requirement which does not override stricter national requirements for a DPO in the relevant Member State (the adopted version).

And:

- *From* a very high threshold where the DPO requirements would only apply to large enterprises with more than 250 employees (Commission's initial proposal), causing the WP29 to complain that the requirement would apply to only 40% of the companies in the EU;
- *… to* a very low threshold whereby a DPO would be required for companies processing personal data of more than 500 individuals per year (Committee on Civil Liberties, Justice and Home Affairs of the Parliament's version) making the requirement to appoint a DPO mandatory for nearly all companies and the threshold being increased to 5000 data subjects in any consecutive 12-month period (Parliament 's version);
- *… and ultimately to* material criteria with no minimum threshold based on number of employees or individuals whose data are processed other than the requirement that the relevant processing activities must be *large-scale*.

Given this history, it is worth discussing the final text in light of the various earlier proposals to see what the

end result has delivered and whether after all of the proposals and fierce debate it is now finally clear when companies are required to appoint a DPO. Spoiler alert: I am not sure it is clear at all, and if we do not get clear guidance from the WP29, the current provision may potentially lead to companies appointing DPOs where it is not warranted.

**The current requirements**

The Data Protection Directive does not stipulate any obligation for controllers to appoint a DPO. Consequently, most of the corresponding national laws of the Member States, for example the UK implementation laws, do not make any mention of a DPO.

Nonetheless, the Directive provides a potential field of application for DPOs with significant practical impact. Under the Directive, as a rule any intended processing operation of personal data requires that the processing must be notified to the national data protection authority. However, Member States are free to allow exemptions from the aforementioned notification duty, *inter alia,* in the case of data controllers that appoint a DPO. As an internal supervisor, a DPO is supposed to ensure compliance with data protection law from within the organisation of the controller, which ultimately warrants a suspension of the preliminary notification duty. This option has been implemented in a number of EEA countries, including Estonia, France, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Poland, Slovakia, Sweden, as well as in Switzerland, where appointment of a DPO is voluntary but can reduce or eliminate an organisation's DPA notification obligations. Instead of notifying the DPA about its data processing systems, the company can "notify" its own DPO about its processing operations, and the DPO will maintain an internal registry. Only a few of the Member States have opted to make the appointment of a DPO mandatory, most notably, these are:

- **Germany**: If more than nine persons are constantly employed in the automated processing of personal data, or if 20 persons or more are employed in non-automated processing of personal data (e.g., HR personnel accessing personnel files).
- **Croatia**: When an organisation has more than 20 employees, it must appoint a personal data "security officer" whose duties incorporate a wide range of data protection-related activities.
- **Hungary**: Appointment of a DPO is mandatory in certain industries only, such as telecommunications providers and financial organisations.
- **Spain**: Appointment of a security officer is mandatory when the personal data processed are subject to "medium-" and/or "high-level" security requirements.

**The GDPR**

The GDPR requires controllers and processors to appoint a DPO when their *core activities*:

- consist of data 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
- consist of data processing on a large scale of special categories of data.

The requirement to appoint a DPO is mandatory in the GDPR, but other than in the initial proposal of the Commission, it *does not* set aside the national requirements of the Member States. This was clearly a concession to Germany in order to overcome its objections to the GDPR taking the form of a regulation and overriding its stricter national requirement of when to appoint a DPO. A group of companies may appoint a

single DPO, provided such DPO is "easily accessible from each establishment." It therefore seems possible to appoint a DPO (which is mandatory under German law) to also function as the "single DPO" for a group of companies under the GDPR.

**What does "large scale" mean, exactly?**

EU legislators have opted for two material requirements relating to types of processing activities without any minimum threshold regarding the number of employees of such company or the number of individuals whose data are being processed. This seems sensible, as it is very difficult to decide in advance whether a DPO is warranted based on the number of employees or the number of individuals whose data are being processed. A manufacturing company can, for example, have a substantial number of employees but perform no invasive data processing whatsoever; on the other hand, WhatsApp had at the time of its takeover by Facebook, only 55 employees and was processing an unprecedented amount of messages of individuals around the globe. Camera systems at a gas station may record visitors well above a threshold of 1500 individuals a year, while the processing itself is not invasive.

EU legislators ultimately settled on a requirement that the processing activities should be "large-scale," which introduces a material threshold rather than an absolute minimum threshold. Note that there is currently little guidance on what large-scale processing means. The GDPR suggests that it means "processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects." However, it does not include the processing of personal data about patients or clients by an individual physician or lawyer (see Pre-amble 91). This guidance leaves a large grey area and therefore provides no guidance at all.

In light of the widely diverting proposals on the minimum thresholds for appointing a DPO in the legislative process, it may well be that the views on what constitutes large-scale data processing for purposes of appointing a DPO may diverge as well, which may currently postpone the discussion rather than solve it.

**What constitutes "core activities"?**

Organisations have to appoint a DPO if their "core activities" consist of regular and systematic monitoring of data subjects on a large scale or of processing sensitive personal data on a large scale (including processing information about criminal offences).

The recitals of the GDPR clarify that the core activities of an entity are a company's primary activities and do not relate to the processing of personal data as an ancillary activity. Thus it is fair to assume that for example, the processing by controllers and processers of their own employee data does not qualify as a core activity, including large-scale processing of special categories of data (e.g., as part of an employee health program) or the regular and systematic monitoring of their employees (e.g., for purposes of data loss prevention). A similar conclusion would be justified if a company monitors wire payments and deposits for anti-money laundering purposes and verifies names against watch lists for anti-bribery, fraud or similar legal purposes, as these types of monitoring are not the core activity of such company, but ancillary.

The elephant in the room, however, is behavioural advertising, which without doubt qualifies as the "monitoring of behaviour of individuals." By now most companies sell their services online and apply some form of behavioural advertising on their websites to tune the content of their websites and on-site advertising

to the preferences of visitors. Advertising networks offering behavioural advertising services to their customers will perform such monitoring as a core activity and this will quickly fall within the definition of "large scale monitoring of individual." But what if a company itself undertakes behavioural advertising to promote its products and services on its own website?

**What constitutes the "monitoring of data subjects"?**

The body of the GDPR does not define "monitoring of data subjects." The criterion is also part of Article 3 of the GDPR, containing the applicability regime of the GDPR. The GDPR is also applicable if a controller or processor is not established in the EU processes where the processing activities are related to "the monitoring of the behaviour" of individuals in the EU "as far as their behavior takes place within the Union."

The preamble of the GDPR relating to the scope of application, suggests that "monitoring of the behaviour of data subjects" refers to an organisation using online means to track and profile a data subject in the EU, particularly to make decisions concerning the data subject or analyse or predict his or her preferences, behaviours and attitudes.

See Preamble 26:

> *In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to make decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*.

Based on this guidance, the logical conclusion would be that monitoring of individuals would likely encompass online behavioural marketing for commercial purposes. Given the fact that most companies offering online services and products by now apply behavioural marketing, the consequence would be that all such companies should appoint a DPO for those reasons only, unless the relevant processing cannot be qualified as *large-scale* (e.g. if the company does not have many website visitors) or would not be considered to qualify as the company's core activity.

To solve the conundrum that all advertising of products and services qualify as core activities, which would lead to a DPO being required for most companies selling products and services online, I suggest the following solution: Whenever a company monitors individuals for purposes of behavioural marketing of its own products and services only, and does not also promote products and services of others and does not provide or sell its data to third parties for behavioural advertising purposes, I find it defendable that the relevant activity is not a core activity of the company as it does not generate its own revenues, but rather ancillary to its core activity of selling it products and services.

This may be different if a company applies behavioural profiling in order to make decisions concerning the individual (e.g., whether to offer a loan or grant a mortgage). In the latter case, profiling becomes an integral part of the offering of the services and products and would qualify as a core activity. The WP29 in its GDPR

action plan has indicated that it will provide guidance on the DPO requirement as one of four priority subjects. Given the substantial obligations and investments required for companies to appoint a DPO, such guidance cannot come quickly enough.

***Lokke Moerel*** *is senior of counsel with Morrison & Foerster and professor of global ICT law at Tilburg University. Since 2004, she heads the working group of chief privacy officers at leading European multinationals who developed a new set of binding data protection rules in consultation with the Dutch DPA, which have since received EU-wide approval.*

*Lokke has written Binding Corporate Rules, published by Oxford University Press in 2012, which is considered the leading textbook on BCR and is further co-authored leading Dutch textbooks on International Outsourcing and Online Advertising. Lokke was recently appointed to the Dutch Cyber Security Council (advisory body of the Dutch cabinet on cybersecurity). She is consistently ranked as a leader in data protection law in Chambers Global and Legal 500.*

*"She has a formidable reputation in the field of data protection, advising numerous blue-chip clients. She is doing market-leading work." (Chambers 2015)*