EU WATCH

DATA PROTECTION AND THE NEW FACE OF PRIVACY COMPLIANCE

*By Jeroen Terstegge**

We are about to have a new type of compliance officer on the block. The soon to be enacted Regulation surrounding Data protection is asking a plethora of questions of organisations active in or within the European Economic Area. Top of that list might be whether or not to appoint a Data Protection Officer but the list continues: to appoint in-house or to outsource, by entity or group, or whether the requirement to appoint should be optional or mandatory – and then, at what level of the hierarchy. The consequences of appointing the wrong individual are severe and this leaves firms and indeed those considering these matters from a broader perspective with something of a dilemma. The Data Protection Officer (DPO) is to be a unique figure in compliance management, as his position, qualifications, tasks and independence are narrowly defined in regulation, leaving organisations little room for maneuver. Some companies already have a (Chief) Privacy Officer (CPO) or DPO, whose current position and tasks may or may not meet those requirements. In this article, Jeroen Terstegge explains the intended requirements of new European Personal Data Protection Regulation which is expected to be enacted in 2014, and from which few will be exempt.

Current requirements

Although the negotiations on the new Regulation in the Council of Ministers and the European Parliament are still in full swing, it is most likely that the final Regulation will include specific requirements for a nominated DPO. The role of the DPO is not new to European data protection law. The position is already mentioned in the current Data Protection Directive 95/46/EC. Some countries, like Germany, Switzerland and Hungary as well as the European institutions, require the appointment of DPO's already.

* **Jeroen Terstegge** CIPP, is executive director of PrivaSense and Editor-in-Chief of *Privacy & Compliance.*

The main incentive for appointing a DPO is the exemption it offers as an alternative to reporting on the organisation's data processing operations to the national Data Protection Authority

Others, like France, Sweden and The Netherlands, have made the position optional.[1] The main inducement for appointing a DPO is the exemption it offers as an alternative to reporting on the organisation's data processing operations to the national Data Protection Authority. Instead the organisation may notify its data processing operations to its own DPO. Other tasks afforded the DPO are supervising the correct application of the Personal Data Protection Act and any applicable sector laws and requirements. Poland and Spain on the other hand, require the appointment of a Data Security Officer (DSO), a position originating from the implementation of the amended ePrivacy Directive. The DSO is responsible for supervising one specific element of the Data Protection brief, namely the correct application of the information security requirements to personal data processed by telecom companies. Although information security is an important *part* of data protection, the scope of the DSO-role is narrower than that of the DPO. The latter not only has supervisory responsibilities with regard to data security, but also with regard to compliance with the other data protection principles: data minimization, purpose specification, collection- and use-limitation, data quality, transparency to the data subject, and the execution of data subject rights.

Who must appoint a DPO?

In order to determine whether the appointment of a DPO is required, organisations should carefully review two types of requirements.

- First, the organisation must determine whether the new Regulation will apply to the organisation and its data processing operations (articles 2 and 3).
- Second, the organisation must determine whether it falls into one of the categories for mandatory DPO's (article 35).

When does the Regulation apply?

According to Article 2, the Regulation applies to all processing of personal data (automated or not) which form, or is

1 http://www.cnil.fr/english/topics/dpo-in-europe/

EU WATCH – DATA PROTECTION AND THE NEW FACE OF PRIVACY COMPLIANCE

intended to form, part of a filing system (the "*material scope*").[2] Most organisations, in both the public and the private sector, will easily fall under the material scope of the Regulation as everyone is using computers nowadays to process information, including personal data of its employees and customers.[3]

Once it has been established that the Regulation is applicable, the organisation must determine whether the Regulation applies to it pursuant to its *territorial scope* (Article 3). The Regulation applies principally anywhere in the European Economic Area (EEA)[4] where the processing of personal data, as a controller or processor of that database, is carried out in the context of the activities of an establishment. Moreover, the Regulation may have extra-territorial application to companies based outside the EEA, where they are offering goods or services to residents of the European Union or where they are monitoring the behavior of residents of the EEA. Where both the conditions of Articles 2 and 3 are met, the Regulation applies to the organisation.

In addition, for some categories of organisations the appointment of a DPO is mandatory (article 35); namely

- all public authorities and bodies;[5]
- companies that employ 250 employees or more; as well as
- companies whose core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic data monitoring.

2 Some entities, such as judicial authorities, have a specific exemption to the Regulation (See art. 2(2)).

3 Contrary to US data privacy laws, which apply to a limited and specified set of data, European data protection law applies to *any* information relating to an identified or identifiable individual. N.B. The Regulation will likely also apply to data which *single out* an otherwise unidentifiable individual such as IP-addresses and cookies.

4 The new Regulation will apply in the 28 Member States of the European Union as well as in Norway, Iceland and Liechtenstein; together, the European Economic Area or EEA. Unofficially, the Regulation is likely to also impact the data protection legislation of the Candidate Countries such as Turkey and Serbia in order to be eligible for full membership. Please note that the Regulation applies directly as soon as it enters into force and does not need to be transposed into national law.

5 In some countries the term "public authority" also includes private enterprises which perform a specific public task (e.g., a garage performing the mandatory automobile safety test1).

The advantage of having a DPO on staff is that he or she is available exclusively to the organisation … (but this) … does not need to be a fulltime position

For all other organisations, the appointment of a DPO is optional. The name of the DPO must be communicated to the Data Protection Authority (DPA) and the public.

In-house, shared or 'outsourcing'?

In most cases, the DPO will be appointed as an employee of the entity which he or she is supervising. However, the Regulation allows for corporate groups and public organisations to designate a Group DPO. Also, the organisation may procure the services of an external company offering DPO services.

The advantage of having a DPO on staff is that he or she is available exclusively to the organisation. Given the broad range of tasks of the DPO (see below), this option may be very attractive to many organisations. Furthermore, the DPO does not need to be a fulltime position. The Regulation allows the DPO to have other tasks and duties as long as they do not result in a conflict of interest. In fact, a recent survey performed by the Dutch DPO Society (NGFG) showed that 75% of all DPO's have other tasks and duties; and 60% of the DPO's indicated that those other duties took more than 50% of their time.[6]

A DPO may also be shared between members of the same group of companies. Many corporations are structured as a group of companies, so they may appoint a single Group DPO. However, the larger the group, the more difficult it is for the DPO to perform his duties well, so the corporation may choose to appoint multiple DPO's instead; one for each group entity, provided such a group entity qualifies for a DPO by itself alone. Public authorities and bodies may also designate a Group DPO, but only where the public authority itself consists of multiple entities. In other words, a Group DPO cannot be appointed to supervise multiple, different public authorities.

Some organisations, especially smaller ones, may opt for an external DPO, as an external DPO is likely to be more cost-effective than an in-house DPO. However, because an external DPO performs his or her duties detached from the organisation, having an external DPO requires extra attention from management to ensure

6 NGFG survey 2013 (not yet published).

Failure to properly involve (an) external DPO exposes the organisation to fines for not having fully complied with the DPO requirements

that the external DPO is included in all relevant projects and decisions. Failure to properly involve the external DPO exposes the organisation to fines for not having fully complied with the DPO requirements (see below). It is therefore important that the service schedule in the contract with the external DPO is well-defined and that the organisation knows when to involve him or her.

Positioning the Role

The Regulation requires that the DPO reports directly to the management of the organisation. Amendments have been tabled which require that the DPO reports directly to the CEO. In any case, it is clear that Europe considers it important that the DPO has direct communication links with senior management. The NGFG survey mentioned above showed that in about 50% of all cases the DPO does not report directly to the CEO, but to another senior manager, such as the Chief Legal Officer. One may safely assume that most of the DPO's currently in Europe are not senior managers, but mostly mid-level managers typically found in amongst general management staff, legal or compliance functions of the organisation. A minority is found in other functions, such as Internal Audit, HR or Finance. This may be logical given the fact that DPO's do not have a responsibility for ensuring compliance with privacy and data protection laws. In its pure form, the DPO role is merely that of the supervisor, playing both the roles of devil's advocate and expert.[7] The responsibility for compliance ultimately remains with management however, and cannot be shifted towards the DPO. Therefore, it is essential that the DPO is taken seriously by senior management[8] and that the he/she has direct access it. Otherwise the DPO-position would merely be a form of window-dressing.

Some companies have appointed C-level executives who carry the title of Chief Privacy Officer (CPO). Essential to note however, is that many of those positions will not meet the requirements

7 In practice, many DPO's are also tasked with (delegated) responsibilities with regard to compliance management, such as the execution of risk assessments, providing training and drafting policies.

8 30% of the respondents in the NGFG survey reported that the organisation did not take them seriously.

The responsibility for compliance (with the Personal Data Protection Regulation) ultimately remains with management and cannot be shifted towards the DPO

of the new Regulation, mainly because of their (often not formalized) duties.

Given the fact that the DPO is required to perform his or her duties independently and may not receive any instructions as to the exercise of his or her duties, the function through which the DPO reports must be carefully considered. Preferably, the independence of the DPO is recognized and defined by a Charter signed by the CEO and co-signed by his or her direct supervisor, so it is clear to everyone that the DPO is independent in the performance of his/her tasks, even when placed in a function not otherwise independent, such as Legal or HR. Where the DPO is part of Internal Audit, the DPO may benefit from the existing Audit Charter governing the independence of Internal Audit (if any), although some modifications may be necessary in order to comply with the Regulation and to avoid any conflicts of interest between functional mandates.

Exercising the Role … or the Function?

A senior executive holding the position of Chief Privacy Officer may seem attractive, especially in complex organisations and organisations with high privacy risk profiles, as the CPO may carry much more (delegated) compliance management responsibilities than a DPO. Often, a CPO supervises specialized staff, including the privacy officers of various divisions and functions of the organisation. It is not yet clear whether this model would be allowed under the Regulation; if the CPO may delegate some of the tasks of the DPO prescribed by the Regulation (see below) to members of his staff; or if a CPO may supervise multiple DPO's (as each DPO should technically be independent, free of instruction). For this reason, some call for the DPO to be a *function* rather than a *person*. This is however not (yet) the way of thinking in Brussels.

Tasks

The DPO has a number of tasks specified by the Regulation (see the box overleaf), although it is allowed to task the DPO with other non-conflicting responsibilities.

This list of tasks shows that the DPO is not only an internal supervisor, but is also deemed to be the internal expert on

DPO REGULATORY DUTIES

- Inform and advise the organisation of its obligations pursuant to the Regulation and document this activity and the responses received;
- monitor the implementation and application of the policies of the organisation in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;
- monitor the implementation and application of the Regulation by the organisation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights;
- ensure that the documentation referred to in Article 28 of the Regulation is maintained;
- monitor the documentation, notification and communication of personal data breaches to the DPA and the data subjects;
- monitor the performance data protection impact assessments and the application for prior authorization or prior consultation of the DPA where required;
- monitor the response to requests from the DPA, and, within the sphere of the DPO's competence, co-operating with such Authority at the latter's request or on the DPO's own initiative;
- act as the contact point for the DPA on issues related to the processing; and
- consult with the DPA, if appropriate, on his/her own initiative.

privacy and data protection, as well as the liaison between the management of the organisation and the DPA. The latter task may put the DPO is an awkward position. At the one hand, as a loyal employee he/she is expected to serve the interests of the organisation. On the other hand, he/she may be seen as part of the DPA. The Regulation even calls upon the DPO to be a whistleblower "if appropriate"! A conundrum and a balance to be found that reflects those of many traditional Chief Compliance Officers already.

Competencies

The Regulation requires that the DPO has (relevant) professional qualities and in particular expert knowledge of data protection law and practices

The DPO may only be dismissed if he or she "no longer fulfills the conditions required for the performance of their duties … The organisation cannot fire a DPO because it does not like the way he or she performs his/her duties"

as well as the abilities to perform the tasks mentioned above. The level of expertise must match the type and complexity of the data processing carried out by the organisation as well as the required level of protection of the personal data. Ergo, the more sensitive the data are and the more complex the organisation is, the better qualified the DPO should be.

The competencies of the DPO must not be underestimated. Generally, the DPO must be a 'Jack of all trades'. Given the many tasks of the DPO set forth by the Regulation, the speed of business and the complexity of the information society nowadays where personal data can be found everywhere inside and outside the organisation, a DPO should at least have (more than basic) knowledge and skills pertaining to the following areas (in no particular order):

- In-depth knowledge of relevant data protection laws and regulations.
- ICT-technology and -design (e.g., cloud computing).
- Information security.
- Audit.
- Compliance management.
- Overall business strategy.
- Ways-of-working of data-intensive business functions (e.g., HR, CRM, Marketing, and R&D).
- Purchasing, outsourcing and M&A.
- Expectations of internal and external stakeholders, such as customers, employees, works councils, DPA's, politicians, the media, etc.
- Internal and external communication.

As the DPO isn't an expert in all of these areas (except in privacy and data protection law as required by the Regulation), it is important that he/she has excellent connections with those in the organisation who are. In some large organisations, this is institutionalized in a group of experts chaired by the DPO, who bring the relevant knowledge to the table and who coordinate overall compliance with privacy and data protection laws and response to privacy incidents and data breaches.

Dismissal

It is worth noting that the Regulation requires that a DPO is appointed for a minimum period of two years and that the DPO may only be dismissed if he

… the mere existence of a DPO already significantly enhances the awareness of privacy and data protection requirements in the organisation

or she "no longer fulfills the conditions required for the performance of their duties" (Article 35(7)). Currently, some countries already have put restrictions on the dismissal of DPO's in their laws. This means that the organisation cannot fire a DPO because it does not like the way he or she performs his/her duties. This makes the selection of the DPO even more precarious. On the one hand, the DPO must have the proper qualifications and must possess the ability to function independently and to be sufficiently critical towards the organisation, on the other hand the DPO shouldn't be someone who is obstructed or ignored by the organisation because of his/her personality or performance.

Sanctions

Non-compliance with the DPO requirements carries a fine of up to 1 million Euro or, in case of a company, 2% of the annual turnover of the enterprise (Article 79(6(j)). It is therefore important that the organisation pays serious attention to the selection as well as the performance of the DPO. Although it is unlikely that a fine will be issued solely for not complying with the DPO requirements, it is highly likely that such non-compliance would be an aggravating circumstance in the event of a breach of any of the material data protection requirements of the Regulation, such as data security, data breach notification and restrictions on data use and data disclosure. After all, as a study by the Dutch Ministry of Justice has shown, the mere existence of a DPO already significantly enhances the awareness of privacy and data protection requirements in the organisation.[9]

Criticism

The Commission's proposal has triggered a lot of criticism from all sides. The most common critique heard is that the criteria for the mandatory DPO are arbitrary. The Commission's choice to put the threshold at 250 employees is inspired by the fact that this is the number used to identify small and medium business (SME's). The Commission is bound by agreements to limit the administrative burden of SME's when proposing new regulations and directives. Therefore, SME's do

9 http://www.wodc.nl/images/1382b-summary_tcm44-165372.pdf

… the degree of risk to the privacy of the individual posed by the organisation is almost never related to its size

not have to appoint DPO's. However, the degree of risk to the privacy of the individual posed by an organisation is almost never related to its size. Very small organisations, especially those which operate online, may pose significant threats to the individual's privacy, where some large industrial organisations may have almost no privacy issues. Several amendments have been tabled to try to come up with better criteria. Furthermore, the Council of Ministers has pledged to make the Regulation more risk-based. This includes the appointment of a DPO. One of the compromise proposals floating in Brussels makes the appointment of the DPO optional, but allows Member States to make the appointment mandatory. This would allow for a serious reduction of the administrative burden associated with the Regulation, while at the same time allowing Germany to protect one of its 'crown jewels' of data protection. We will have to see the final outcome of the negotiations (expected in 2014) to know the exact criteria. ■

Jeroen Terstegge CIPP, is executive director of PrivaSense, a consultancy firm in privacy and data protection law and compliance management, and Editor-in-Chief of *Privacy & Compliance*. Before that, he was Corporate Privacy Officer with Philips. He can be reached via www.privasense.eu or @PrivaSense.

SUBSCRIPTION INFORMATION

Subscription prices

FTE's	Corporate	Universities
Personal subscription		
1 Hard Copy (6 issues)	€ 195	€ 195
Institutional subscription		
3 Online users +1 Hard copy	€ 450	€ 450
5 Online users + 5 Hard copies	€ 550	€ 450
10 Online users + 10 Hard copies	€ 750	€ 450
>10	To be negotiated	€ 450

* Online access includes the complete archive

Please go to our website for the general information regarding our journal subscriptions.
http://www.baltzersciencepublishers.com

New Subscriptions

Subscriptions start with the first announced issue of the calender year. If subscriptions are started in the course of the calender year the full subscription rate applies, and the subscriber will get full access to the archive of the journal.

Change of address

Please mail your change of address to the address mentioned on the contents page, or consult the website.

Terminating a subscription

Subscriptions can only be cancelled, by email or letter, until 1 December of the present subscription year. After this date subscriptions will be automatically renewed for the following year.

ISSN: 2211 8934 • E-ISSN: 2211-8942

Subscription Information

Details on subscription rates and offers are available on request from the publisher.

Advertising Rate Card

2012 prices, excluding applicable VAT.

Full page

1x € 1000
5x € 750 (per page)

Half page

1x € 600
5x € 450 (per half page)

For technical instructions please contact the marketing/sales department:
info@baltzersciencepublishers.com