Centre for Information Policy Leadership
Hunton & Williams LLP

The Role and Function of a Data Protection Officer in the European Commission's Proposed General Data Protection Regulation

Initial Discussion Paper

25 September 2013

1. Introduction

The data protection officer ("DPO")[1] is an essential component of a data privacy accountability framework, playing a crucial role in enabling organisations to ensure, and to demonstrate, data privacy compliance. Unsurprisingly, the role of the DPO is formally recognised by and described in detail in the General Data Protection Regulation proposed by the European Commission (the "Regulation").[2] This initial discussion paper examines the requirements for the appointment of a DPO and the nature, function and scope of the DPO role, as envisaged by the Regulation.[3] The paper also identifies key issues and challenges arising from the current proposal that may benefit from further consideration.

This discussion paper launches a project by the Centre for Information Policy Leadership[4] (the "Centre") to explore the changing role and function of a DPO and the implications of this for organisations, individual DPOs and data protection supervisory authorities ("DPAs"). If you would like to participate in the Centre's project, please contact Bojana Bellamy at bbellamy@hunton.com.

2. Executive Summary

The role and function of the DPO has evolved in recent years but has not previously been mandated within the general EU data protection framework. The proposed Regulation requires a DPO to be appointed when certain threshold criteria are met, sets out requirements for the appointment of a DPO, describes key areas of responsibility and lists specific tasks. Irrespective of whether the appointment of a DPO remains a mandatory

---

[1] The terms DPO and CPO ("Chief Privacy Officer") are used interchangeably in this paper.

[2] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published January 25, 2013. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed Aug. 14, 2013).

[3] It also takes into account relevant amendments proposed by the Presidency of the Council of the European Union and the responsible committees of the European Parliament, namely, the Committee for Civil Liberties, Justice and Home Affairs ("LIBE" – lead committee), the Committee on Employment and Social Affairs ("EMPL"), the Committee on Internal Market and Consumer Protection ("IMCO"), the Committee on Legal Affairs ("JURI"), and the Committee on Industry, Research and Energy ("ITRE").

[4] © 2013 The Centre for Information Policy Leadership LLP. The content of this paper is strictly the view of the Centre for Information Policy Leadership and does not represent the opinion of either its individual members or Hunton & Williams LLP. The Centre does not provide legal advice. These materials have been prepared for informational purposes only and are not legal advice, nor is this information intended to create an attorney-client or similar relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Please do not send us confidential information. Visit us at www.informationpolicycentre.com. For more information about this project please contact Bojana Bellamy at bbellamy@hunton.com.

requirement, the Regulation sets out clear expectations for the role, and underscores its significance in a wider data privacy accountability context.

Much of the thinking in the Regulation codifies the practices that have evolved in organisations with a mature data privacy function and reflects the increased sophistication of the DPO role. [5] However, there are aspects of the new requirements that would benefit from further analysis and discussion. For example, the DPO's protected employment status, and the need for the DPO's other responsibilities to be compatible with the role of a DPO will inevitably raise conflicts of interest. The requirement for the DPO to report to management and yet to be independent and consult generally with DPAs will likely raise further conflict concerns. A framework for resolving these conflicts should be considered. The Regulation envisages that the DPO will have an essential and strategic role in ensuring accountability and overseeing an effective privacy compliance programme. Yet analysis of the different roles the individual might have, their place within the organisation, their required skill set, relationship with management and with the business, and the ethical dimension of the role, remain at an early stage.

3. The Requirement for a DPO under the Regulation

The Regulation mandates the appointment of a DPO in certain circumstances and prescribes the nature, function and scope of the role.[6] Few existing national laws that implement the current EU Data Protection Directive (Directive 95/46/EC) mandate the appointment of a DPO. Notable exceptions are Germany,[7] the Slovak Republic,[8] Slovenia,[9] and Poland.[10] In a number of EU Member States, including Estonia, France, Latvia, Luxembourg, Malta, the Netherlands, and Sweden, the optional appointment of a DPO can reduce or eliminate an organisation's notification obligations with the local DPA. The Regulation would introduce a general, EU-wide obligation (possibly subject to minimum threshold requirements) to appoint a DPO. The Regulation would take direct effect in all 28 Member States and would replace and harmonise existing national law requirements relating to the role and responsibilities of a DPO.

4. Appointment of a DPO

The Regulation prescribes a number of minimum requirements for the appointment of a DPO, described below.

4.1 *The duty to appoint a DPO applies to both controllers and processors.* [11]

[5] As witnessed by the growth in professional networks of DPOs, and the global growth of the International Association of Privacy Professionals.

[6] The substantive provisions are set out in the Regulation at Chapter IV – Controller and Processor, at Section 4 - Data Protection Officer. These provisions cover the designation (Article 35), position (Article 36), and tasks of the DPO (Article 37) (*see* Annex I for the relevant extract from the Regulation).

[7] Generally required where the data controller processes personal data by automatic means and has nine or more employees.

[8] Generally required where the data controller has 20 or more employees.

[9] Generally required where the data controller has 50 or more employees.

[10] Polish data controllers are generally required to appoint an administrator of information security, not wholly dissimilar to a DPO but having a more restricted scope, focussed largely on security.

[11] Regulation, Article 35(1).

This requirement raises issues of potential conflict and practical difficulties - where the processor carries out processing tasks on the controller's behalf, the DPO of both the controller and the processor would each carry out monitoring and oversight tasks in relation to the same processing activity. The DPOs would need to work together to allocate statutory responsibilities between them, specify the scope of their respective roles and potentially retain some overlapping duties.

4.2 *All public bodies must appoint a DPO.* [12]

Where the controller or processor is a public body, a single DPO may be appointed for several entities, departments and/or agencies. The requirement to appoint a DPO within the public sector reinforces the view that public sector bodies have increased accountability requirements and must ensure and demonstrate compliance with data privacy laws, as in the private sector.

4.3 *Private and other non-public sector organisations (e.g., not-for-profit) must appoint a DPO where they meet certain threshold requirements:* [13]

a) They employ at least 250 people. [14]

   The requirement to appoint a DPO where an organisation has more than 250 employees, without any reference to the potential risk of the processing that may take place, is in contrast to harms-based and risk-based approaches to regulation.

   Amendments proposed by the European Parliament and the Council of Ministers seek to address this.

   The draft report[15] of the lead Parliamentary Committee (LIBE) proposes amendments to the applicable threshold by focusing on the number of affected individuals (500), rather than the number of employees. Similar amendments proposed by the EMPL Committee would mandate the appointment of a DPO where an organisation processes personal data relating to 250 or more data subjects. Amendments proposed by the Council of Ministers under the Irish Presidency would remove all appointment thresholds and make the appointment of a DPO optional, rather than mandatory.

b) Their core activities involve data processing that require regular and systematic monitoring of individuals. [16]

   There is no further guidance on the types of processing activities that would fall within the scope of this requirement but it could potentially be extensive. Under amendments proposed by the LIBE Committee, the requirement to appoint a DPO

[12] Regulation, Article 35(1)(a).
[13] Regulation, Article 35(1)(b) and (c).
[14] Regulation, Article 35(1)(b).
[15] First draft report of the LIBE Committee, published on January 16, 2013. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fEN (last accessed Aug. 14, 2013).

[16] Regulation, Article 35(1)(c).

would apply also where the organisation's processing activities involve profiling or processing of special categories of personal data (e.g., sensitive personal data). [17]

4.4 *A group of undertakings may appoint a single DPO for the group.* [18]

This is a welcome approach and reflects current practice in many organisations that already appoint a European DPO. It is not clear, however, whether the DPO may be located outside of the EU. Also, it may be difficult for a single DPO to successfully fulfil his/her statutory duties under the Regulation in relation to all applicable national laws, where national divergences remain (e.g., in the areas of employment law and freedom of speech).

4.5 *The DPO may be an external contractor and need not be a permanent employee of the organisation .*[19]

This provision would alleviate administrative burdens for SMEs, but it raises the question of whether, by appointing an external DPO, an organisation can fully and effectively comply with its obligations under the Regulation, in particular, the accountability obligations under Article
22. Further, organisations will need to assess whether an external DPO could successfully discharge all of the statutory tasks of the DPO role as envisaged under the Regulation. The appointment of an external DPO may also raise issues of confidentiality and conflict of interests for both the organisation and for the external DPO.

4.6 *Organisations must communicate the contact details of the DPO to the supervisory authority and to the public.* [20]

The identity of the relevant supervisory authority should be clarified. At present, it is not clear whether this would be the supervisory authority of the main establishment, or the supervisory authority in every Member State in which the organisation's controllers and processors operate.

Under amendments proposed by the LIBE Committee, where an organisation decides not to appoint a DPO, it must communicate its reasons to the supervisory authority. [21]

Otherwise, the appointment of a DPO is optional. In those circumstances, it appears that if an organisation formally appoints a DPO in circumstances where there is no legal obligation to do so, the DPO would have the same statutory duties and rights as the mandatory DPO. The position is less clear where a member of staff is allocated responsibility for data privacy compliance in addition to other duties. In practice, organisations may wish to ensure that there is no ambiguity where a member of staff is merely allocated responsibility for data privacy compliance as one of a number of areas of responsibility, but not formally appointed as a DPO. There may be scope for dispute and

[17] LIBE amendments to Regulation, Article 35(1)(ca).
[18] Regulation, Article 35(2).
[19] Regulation, Article 35(8).
[20] Regulation, Article 35(9).
[21] LIBE amendments to Regulation, Article 35(9).

the staff member may seek to benefit from the statutory rights, in particular, protection from dismissal.

5. Features of the DPO Role

5.1 *Organisations must take into account the required professional skill, level of expert knowledge, and the candidate's ability to fulfil the tasks allocated by the Regulation .*[22]

The level of required expert knowledge should be determined by the employer, having regard to the nature of the processing carried out and the required level of data protection. The expected level of expertise may be unrealistically high. Where an organisation operates in multiple EU Member States and appoints a single DPO, the DPO would need to demonstrate relevant expert knowledge of each Member State's data protection law (e.g., local differences legislated for under Chapter IX[23] or requirements for prior consultation in individual Member States under Article 34(4)). The DPO would also be expected to demonstrate relevant experience of how the laws operate in practice (e.g., the inevitable local differences in approach between supervisory authorities, and the cultural expectations of local data
subjects).

5.2 *The DPO must be appointed for a term of at least two years, and can be re-appointed.* [24]

A short or fixed term of tenure may run contrary to current corporate practices and the needs of organisations. The DPO role is an integral part of a corporate governance structure and data privacy compliance is an on-going task that requires continuity, consistency and leadership. It may be unrealistic to expect a DPO with a fixed two year term to successfully ensure compliance with the Regulation, in particular the accountability requirements of Article 22. Organisations likely would face an unnecessary administrative burden to recruit candidates every two years, especially given that market demands for suitable candidates will almost certainly exceed the number of available candidates.

Under amendments proposed by the LIBE Committee, the DPO would be appointed for a term of four years, but could not be re-appointed after the expiry of that term. This prohibition on re-appointment could raise similar issues for organisations as discussed above. Amendments proposed by both the JURI Committee and the Council of Ministers would remove the requirement for a minimum two year period of tenure.

5.3 *The DPO has protected employment status and cannot be dismissed, unless they no longer fulfil the conditions required for performance of their duties.* [25]

This may present practical difficulties both for individual DPOs and organisations. Organisations have complex internal performance management and review processes, frequently based on set criteria and quotas. It is possible that a DPO may not meet

[22] Regulation, Article 35(5).
[23] Regulation, Articles 80 (freedom of expression), 82 (employment), 84 (obligations of secrecy), 85 (churches and religious associations).
[24] Regulation, Article 35(7).
[25] Regulation, Article 35(7).

internal performance criteria, yet still be a good DPO and perform all the tasks envisaged by the Regulation. Values and criteria for good performance will differ from one organisation to another and may conflict with the expectations of DPAs and the specific tasks of the DPO prescribed by the Regulation. This may place DPOs in a difficult or untenable position. For example, a DPO who prevents a new product or service being launched based on data privacy compliance objections might be deemed a poor performer, yet s/he may have met the obligations of a DPO, but fail to meet other reasonable and legitimate requirements of the employer, such as: cooperation and team working; the ability to communicate clearly; understand related issues, including interconnected legal obligations (e.g., contract and employment law) and commercial considerations.

5.4 *Other professional tasks of the DPO must be compatible with the DPO's role and not result in a conflict of interests.* [26]

This requirement may limit the DPO's ability to perform other tasks and may exclude part-time DPO roles. Organisations would need to consider carefully where to position the DPO within the organisation's structure. For example, the role may not sit comfortably within the legal function, as the duties of a legal advisor are different and could conflict with those of the DPO, as envisaged by the Regulation. Similarly, the DPO role could conflict with the information security function, as information security measures and technology frequently raise data privacy compliance challenges but the priorities of the information security function may be different from the priorities of the DPO.

There appears to be some experience of these issues in Germany. The Düsseldorfer Kreis, which has provided guidance on the role of the DPO under German law, has identified a number of roles that are incompatible with the role of the DPO, for example HR Director, or IT Director.

5.5 *The DPO must report directly to the organisation's management, must be guaranteed a degree of independence and must not be required to take instructions regarding the exercise of his/her functions.* [27]

The independence of the DPO is enhanced by requiring the DPO to act as a contact point for and to cooperate and consult with the supervisory authority, including on the DPO's "own initiative".[28] That said, the requirement for independence and direct reporting to senior management may create an inherent conflict of interests for the DPO. An employee's loyalty typically lies with the employer, and employees frequently are shareholders in the business. There is a risk that by positioning the DPO as autonomous and independent, the DPO will not be fully integrated into and involved by the organisation. In particular, there is a risk that the DPO may even be viewed internally with some suspicion, and deliberately (or subconsciously) distanced. This would prevent the DPO from being able to properly advise the organisation, or discharge the statutory requirements of his/her role. This could have particular implications for new projects, products and services, which trigger new obligations of privacy by design and

[26] Regulation, Article 35(6).
[27] Regulation, Article 36(2).
[28] Regulation, Article 37(1)(h).

privacy by default, under the Regulation. A DPO can add most value by being involved in new initiatives from the outset, embedding data privacy advice and compliance steps early in the design of new products and services.

Experience of organisations with comprehensive and mature data privacy compliance programmes suggests that the more successful and better integrated corporate privacy management programmes may be those in which data privacy compliance is embedded in every aspect of the business, accountability is shared across business functions and the DPO is seen as a business enabler, guardian and trusted advisor, rather than a policeman and enforcer.

Global organisations that currently appoint central DPOs or CPOs outside of the EU will have to carefully consider EU requirements for direct reporting lines and independence. They may find that EU based DPOs cannot report directly to a group DPO/CPO based outside the EU, or be directed by foreign supervisors. This may ultimately constrain an organisation's ability to ensure effective data protection oversight and accountability through a single corporate privacy compliance and management programme.

5.6 Organisations must provide support to the DPO, including staff, premises, equipment, training and any other resources necessary to carry out the tasks allocated to him/her. [29]

This requirement recognises the reality that data privacy accountability and effective oversight can only be achieved with appropriate resources and support from senior management. It may also result in DPOs having to undergo regular training and gain a professional certification, such as that already offered by the International Association of Privacy Professionals.

5.7 *Organisations must involve the DPO "properly and in a timely manner" in all issues that relate to the protection of personal data.* [30]

Organisations will need to put in place procedures and instructions to all staff and business functions to engage the DPO in every matter of internal data privacy compliance. Further, DPOs will need to ensure they have sufficient staff and resources to be able to respond to and deal with each internal query appropriately and promptly.

5.8 *Individuals have the right to contact the DPO on all issues relating to the processing of their data and to request the exercise of their rights under the Regulation.* [31]

In addition to a significant internal role, the DPO would also have an external-facing role. As a spokesperson for or the "face" of the organisation, the DPO will need to be suitably experienced in handling public relations. Furthermore, if organisations use an external contractor as their DPO, they will need to impose clear contractual requirements regarding external communications made on behalf of the organisation.

[29] Regulation, Article 36(3).
[30] Regulation, Article 36(1).
[31] Regulation, Article 35(10).

The Regulation implies that the DPO will have a role as ombudsman in the event of complaints and disputes. This role, together with the more general requirement of independence may raise issues of conflicts of interests within the organisation when the DPO handles complaints or deals with the exercise of individuals' rights. [32]

6. Tasks of the DPO

The DPO is required to undertake the following tasks: [33]

6.1 *Information and advice.* [34]

The DPO informs and advises the organisation of its obligations under the Regulation, and documents this advice.

6.2 *Oversight and monitoring.* [35]

The DPO oversees and monitors the implementation of the organisation's data protection compliance programme and the organisation's compliance with the Regulation.

The specific tasks would include: monitoring the implementation and application of internal data protection policies; assigning responsibilities; providing staff training; conducting audits; monitoring the implementation of data protection by design and default, data security, and the rights of data subjects; monitoring documentation, notification and communication of personal data breaches; monitoring the performance of data protection impact assessments and applications for prior authorisation or prior consultation.

6.3 *Administration and documentation.* [36]

The DPO ensures that the documentation requirements under the Regulation are maintained.

6.4 *Consultation and cooperation with data protection authorities.* [37]

The DPO acts as the contact point for the supervisory authority, cooperates with the supervisory authority and consults with the supervisory authority on the DPO's own initiative.

Amendments proposed by the Council of Ministers would narrow the scope of the DPO's responsibilities by excluding the requirement to monitor the implementation and application of the Regulation, the documentation requirements, breach notification, and the conduct of DPIAs.

[32] Regulation, Article 35(10).
[33] Regulation, Article 37(1)(a)-(h).
[34] Regulation, Article 37(1)(a).
[35] Regulation, Article 37(1)(b).
[36] Regulation, Article 37(1)(d).
[37] Regulation, Article 37(1)(g) and (h).

7. Conclusion

The development of the role of the DPO has been a striking feature of the last decade of data protection regulation and corporate risk management. The expectations of the DPO role are increasing, both in practice and in law. The detailed description in the Regulation of the role and tasks of a DPO provides a comprehensive starting point for discussion. However, it also raises practical questions as to how the role will work and how it should be designed to ensure that the DPO is the strategic cornerstone of accountability and data privacy compliance, and continues to balance the increasingly complex interests of organisations, individuals and data protection supervisory authorities.

Annex I

Extract from the Regulation

SECTION 4
DATA PROTECTION OFFICER

Article 35

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

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

   b) the processing is carried out by an enterprise employing 250 persons or more; or

   c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for

further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

Article 36

Position of the data protection officer

1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Article 37

Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

   a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

b) to monitor the implementation and application of the policies of the controller or processor 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;

c) to monitor the implementation and application of this Regulation, 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 under this Regulation;

d) to ensure that the documentation referred to in Article 28 is maintained;

e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer’s own initiative;

h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.