Centre for Information Policy Leadership
Hunton & Williams LLP

The Data Protection Officer

in the

General Data Protection Regulation

Draft Discussion Paper for Paris GDPR Workshop II

19 September 2016

12 September 2016

Table of Contents

Executive Summary

The data protection officer ("DPO") is an essential component of data privacy accountability, playing a crucial role in enabling organisations to ensure and demonstrate data privacy compliance and effective privacy protection to individuals. In recognition of its crucial status within organisations, the role of the DPO is formally recognised by and described in detail within the General Data Protection Regulation ("GDPR") and, thereby, for the first time, formally mandated within the EU data protection framework.

This CIPL paper on the "Data Protection Officer in the General Data Protection Regulation" examines the requirements for the appointment of a DPO and the nature, function and scope of the DPO role under the GDPR. While the GDPR outlines key parameters and sets clear expectations for the DPO role, underscoring its significance in a wider data privacy accountability context, there are a number of areas that present challenges, or require clarification, interpretation and guidance to ensure an effective implementation of the DPO role. This paper examines these areas and makes suggestions regarding implementation and interpretation as well as further guidance by the WP29.

With respect to the criteria of "systematic" and "regular" and "large scale" processing as precursors to the **mandatory appointment of a DPO**, organisations will require a clear and concrete understanding of these terms in order to meet their obligations under the GDPR. CIPL takes the view that companies should be able to determine whether their processing operations fall within the ambit of the "systematic-large-scale-regular" criteria using their best judgment and taking into account their whole business operations. Organisations should also be able to identify and demonstrate their decision-making process on this matter in the event of an inquiry or enforcement action by an EU DPA. Thus, any WP 29 guidance might focus on a set of factors that might be considered to assist companies in determining whether they fall within the "systematic-regular-large scale" criteria.

The appointment of a **voluntary DPO** is another key area requiring clarification and guidance. While organisations that do not meet the criteria of a mandatory DPO appointment are under no obligation to appoint a DPO, CIPL believes that in order to discharge their general obligations under GDPR, including implementing accountable and effective data privacy compliance programmes, organisations will have to allocate responsibility for their data privacy and GDPR compliance to one or more dedicated employees who may or may not carry the DPO title. Thus, organisations should be encouraged to appoint DPOs or employees with an equivalent role. However, a potential obstacle may be that it is unclear whether voluntary DPOs will be held to the same standards as mandatory DPOs. As a matter of best practice, therefore, CIPL recommends, that voluntary DPOs should not be subject to the same GDPR DPO requirements as a mandatory DPO so as to not disincentivise the appointment of voluntary DPOs.

The DPO role encompasses strategic and governance functions rather than merely a compliance function. This has been reflected in its evolution from initial beginnings as a side bar role within legal or compliance departments to its currently more typical position directly under or at the executive level. The evolution along this trajectory towards a more complex strategic and governance role has also resulted in a body of "best practices" for the DPO role. These should be taken into account when implementing the DPO role under the GDPR.

The GDPR does not specify the required **"…professional qualities" and "expert knowledge of data protection law and practices"** of the DPO. CIPL recommends that the appointment of DPOs should be based on the specific requirements and needs of an organisation in terms of the skills and qualities required to fulfill the role of DPO. Some specifics are best left to the personnel departments and hiring managers of organisations in searching and selecting the most suitable person for the DPO role.

The DPO guidance should clearly establish that the DPO role should encompass both the DPO office holder and supporting DPO staff to assist the role holder to discharge his or her responsibilities to the organisation, the individual and the regulators. This should also encompass the ability to access and rely on the knowledge, expertise and counsel of other internal and external resources to discharge the function of DPO. While a DPO role encompasses legal knowledge and experience for its advisory tasks, it also includes other areas of expertise and skillsets outside of the data privacy or even legal arena, as specified in this paper. CIPL recommends against requiring that the DPO role should necessarily be held by an individual with a legal background.

A striking feature of the DPO GDPR provisions is the requirement for the DPO to report directly to the **"highest management level"**. This requires interpretation by the WP 29. We believe the reporting lines for a DPO should be true reporting lines, mapping a DPO's report to the appropriate management level where significant strategic influence and authority is held with respect to the DPO's tasks.

Further, the DPO duties of confidentially or secrecy as detailed under article 38(5) could potentially create conflict if a DPO, who is expected to discharge his or her duties to an organisation in a cooperative and transparent manner, is expected to operate under a shroud of secrecy per the GDPR text. We recommend a broad interpretation of this provision to create a workable and sensible solution as to the types of information that should be kept confidential by a DPO vis-à-vis the company.

The issue of "**conflict of interests"** also requires clarification under article 38(6). While the provision does not prevent a DPO from fulfilling other non-DPO duties, an employer does have a duty to ensure that the DPO and non-DPO duties do not conflict. We believe a wide interpretation should be taken of the roles and duties that are found to be compatible with the DPO function. Industry experience demonstrates that Chief Privacy Officers successfully combine their roles with other roles, such as information governance officer and chief data strategist. It is the very essence of a successful DPO to have a wide-ranging and diverse skillset and to perform multiple interdependent functions within an organization, including compliance, business strategy and governance functions.

Under the GDPR, DPOs will have an obligation to **"consult"** with EU DPAs where appropriate on relevant data protection matters. The scope of this obligation is currently unclear and we would call on further WP29 guidance on this to ensure that the "consultation" envisaged by the GDPR text is interpreted to support the role of the DPO both as a credible and trusted business advisor within the organisation and a trusted organisational representative to the relevant DPA.

The development of future WP29 guidance on the DPO will provide a vital opportunity to clarify and expand on the important role of the DPO so that the role can be discharged effectively. Such guidance should preserve the maximum flexibility possible to organisations to implement the DPO role as appropriate within their contexts and circumstances, taking into account their organisational structure, culture and data privacy strategy. This becomes particularly important for SMEs, non-profits, NGOs and universities that may have extensive processing operations but limited resources.

1. Introduction

1.1 The DPO Role in the Data Protection

In recent years, there has been an increasing recognition of the role of the data protection officer ("DPO") in enabling companies and institutions to meet their data protection compliance and accountability obligations as well as protecting the fundamental rights and freedoms of individuals.

Currently, European member states inconsistently approach the role of the DPO. For example, countries, such as Germany,[1] the Slovak Republic,[2] Slovenia,[3] Poland[4] and Spain, mandate the appointment of DPOs in specific circumstances. Other countries, such as Estonia, France, Latvia, Luxembourg, Malta, the Netherlands and Sweden, give to companies the latitude to appoint voluntary DPOs to reduce the organisations' notification obligations to the relevant European data protection authority ("EU DPAs").[5] Relatedly, European institutions also have the obligation to appoint DPOs in particular circumstances.[6]

The General Data Protection Regulation ("GDPR")[7] has explicitly recognised that DPOs are useful and necessary components of an effective data privacy accountability and compliance program. Articles 37-39 thereof deal with designation of the DPO, the position of the DPO, and set forth the DPO's responsibilities regarding their information, advisory, monitoring, co-operative, consultation and points of contact tasks.[8]

1.2 The CIPL GDPR Project

This paper is produced by the Centre for Information Policy Leadership at Hunton & Williams LLP ("CIPL") as part of its project ("CIPL GDPR Project") on the consistent interpretation and implementation of the GDPR.

The CIPL GDPR Project – a two-year long project launched in March 2016 - aims[9] to establish a forum for an expert dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the Member States and academic experts on the

[1] Generally required where the data controller processes personal data by automatic means and has nine or more employees. [●]
[2] Generally required where the data controller has 20 or more employees. [●]
[3] Generally required where the data controller has 50 or more employees. [●]
[4] 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, focused largely on security. [●]
[5] The Netherlands has developed a checklist to help companies to decide whether or not to appoint DPOs. See NGFG (2008, April), Am I the lucky one? Den Haag, the Netherlands.
[6] Regulation (EC) 45/2001, art. 24 (1). [Need to insert a line about implementation].
[7] Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the EU, L 119/1.
[8] Article 39; *see also* Section 7 (Tasks of the DPO).
[9] The objectives of the CIPL GDPR Project are set out in Appendix 1.

consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and reports.

The CIPL GDPR Project focuses on five topics, namely:[10]

a. Data privacy programmatic management;

b. Core principles and concepts;

c. Individual rights;

d. International data transfers; and

e. The relationships of and with EU DPAs, enforcement and sanctions.

As part of the CIPL GDPR Project work plan for 2016,[11] CIPL aims to provide input to the Article 29 Working Party ("WP29") on three of its priority areas[12], namely, DPOs, certification as well as "high risk" and data protection impact assessments. This paper on DPOs is an elaboration of topic a.

1.3 CIPL's DPO Paper

In this paper, CIPL aims to provide the **WP29** and **data privacy practitioners** with input on **DPOs** as follows.

a. Identifying and analysing the relevant GDPR provisions on the appointment, "personhood" (whether the DPO can be a natural and/or legal person), liability, employment status, knowledge, skills, independence, secrecy or confidentiality obligations and tasks of the DPO as well as the obligations of companies to DPOs (e.g. proper and timely involvement in data protection matters, provision of access to resources and "no conflict" obligation).

b. Evaluating the interpretational gaps in the GDPR DPO provisions and assessing the potential challenges which some organisations may face when implementing such provisions. CIPL will suggest potential areas where WP29 guidance may assist companies in handling these implementation challenges.

c. Suggesting potential solutions to the interpretational and implementation challenges. CIPL will draw from its previous work on the role of the DPO[13] as well as the DPO experience in relevant European jurisdictions and European and global companies.

---

[10] See Appendix 2.

[11] See Appendix 3.

[12] Article 29 Working Party, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), WP236, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

[13] CIPL, "The Role and Function of a Data Protection Officer in the European Commission's Proposed General Data Protection Regulation," (2013), *available at*

d. Suggesting "best practices" for the appointment and role of the DPO to ensure the effectiveness of the DPO role in the GDPR context (e.g. driving organisational accountability and protecting the fundamental rights and freedoms of individuals), taking the position that the DPO role is a strategic and governance role rather than merely a compliance role.

2. Appointment of DPOs under the GDPR

In this section, we analyse the main GDPR provisions which apply to the appointment of DPOs.

2.1 Appointment of Mandatory DPOs

Article 37(1) of the GDPR provides that both controllers and processors[14] have a duty to appoint a DPO in certain cases. The processor's obligation to appoint a DPO is consistent with the heightened legal obligations of processors under the GDPR, with many GDPR provisions now directly applicable to processors.[15]

The GDPR provides that companies that fail to comply with all their mandatory DPO obligations (including appointing a DPO and meeting their GDPR obligations to DPOs[16]) will be "subject to an administrative fine of up to 10,000,000 EUR, or up to 2% of annual global revenue, whichever is higher."[17] As written, such penalties appear to apply regardless of any injury to the relevant individuals, compliance with other GDPR provisions or the presence of an otherwise effective data privacy management program within the organisation. However, the appropriate execution of the mandatory and non-mandatory[18] DPO role should be a mitigating factor, when considering the appropriate sanction

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_dpo_in_the_eu_commissions_proposed_general_data_protection_regulation__discussion_paper_.pdf; CIPL, "The Role and Function of a Data Protection Officer in Practice and in the European Commission's Proposed General Data Protection Regulation: Report on DPO Survey Results," (2015), *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_a_dpo_in_practice_report_on_survey_results.pdf.

[14] Article 4(7) of the GDPR defines a "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." Article 4(2) of the GDPR defines "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Article 4(1) of the GDPR defines "personal data" as "any information relating to an identified or identifiable natural person…an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person…". Article 4(8) of the GDPR defines a "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

[15] E.g., Articles 3(2), 27, 28, 30, 31, 32, 33 and 37, GDPR.

[16] See Section 6.

[17] Article 83 (4)(a), GDPR.

[18] See Section 2.2.

in cases where a company has breached other aspects of the GDPR rather than a stand-alone item for purposes of administrative fines.

As analysed next, the GDPR provides for **mandatory appointment of a DPO** in **four cases**.

a. If the processing is carried out by a public authority or body

Article 37(1)(a) contains the requirement to appoint a DPO if the processing is carried out by a public authority or body. This provision does not apply to courts that are acting in their judicial capacities. Under the GDPR, just like private companies, public sector bodies or authorities must implement and be able to demonstrate effective data protection programmes. The GDPR makes it possible for public authorities or bodies to appoint a single DPO for several such authorities or bodies, taking into account their organisational structure and size.[19]

In our view, this provision covers private sector controllers and processors that provide personal data processing services to a public authority or organisation. Where a processor provides services to public authorities or organisations and private sector controllers, the processor should only have the obligation to appoint a DPO in respect of its activities for the public authorities or bodies.

b. Where the "core activities" of controllers and processors consist of "…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"[20]

This ground raises several **interpretational difficulties** which could be addressed by the **WP29.**

- What are the **meanings of the terms "systematic" and "regular" and "large scale"**? Are these criteria objective or subjective and how can they be further clarified? This requires further clarification.

  In addition, the interpretation of the "systematic-large scale-regular" criteria in Article 37 should be consistent with other provisions in the GDPR that outline obligations in relation to "high risk" processing. In other words, the "systematic-large scale-regular" criteria are a specification of the notion of high risk. It should be clarified whether organisations that undertake the types of "large-scale and "systematic" processing operations requiring a data protection impact assessment according to Article 35(3) of the GDPR automatically have an obligation to appoint a mandatory DPO.

- Generally, CIPL takes the view that companies should, within the limits of Article 37, have a discretionary margin to determine whether their processing operations fall within the ambit of the "**systematic-large-scale-regular" criteria** using their best judgment and taking into account their whole business operations. Organisations should also be able to identify and demonstrate their decision-making process on this matter in the event of an inquiry or enforcement action by an EU DPA. Thus, any WP 29 guidance should focus on a set of factors that might be considered

[19] Art. 37(3), GDPR.
[20] Art. 37(1)(b), GDPR.

to assist companies in determining whether they fall within the "systematic-regular-large scale" criteria.

- It follows from the text of Article 37(1)(b) that the **"systematic-regular-large scale" criteria** should be applied **cumulatively**. This means that monitoring must be "systematic", "regular" and "large scale" to trigger a mandatory appointment of a DPO.

- **Sporadic, one-off cases of monitoring, or monitoring of smaller groups of individuals** would not fall within these criteria. Examples of this may include monitoring of account holders who are in default by financial institutions or flagging customers for fraud or money laundering. However, the "core activities" of social media platforms, location based apps, search engines, or email providers may often imply systematic, regular and large-scale monitoring of individuals by the very nature of the service provided.

- The relevant GDPR provision and Recital states that the **"regular-systematic-large-scale" test** applies only to the **"core activities"** of the controller or processor.[21] Recital 97 clarifies that the "core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities." Accordingly, any monitoring of activities that are ancillary to such core activities, such as processing of employee data, monitoring of employees or other parties on company premises and monitoring of company emails, assets and systems, would not fall within the ambit of the mandatory DPO provision. In contrast, companies which develop new lines of business that "monetise" personal data are likely to meet the mandatory DPO requirement. However, companies which use analytics tools to understand how their customers use their online products and improve their products should not be considered as engaging in "systematic-regular-large-scale" activities that trigger the mandatory appointment of a DPO. These types of activities are necessary for many businesses so that they can improve their products and remain competitive.

- The GDPR does not contain guidance on how the **"core activities" of processors** can be determined. However, the guidance set out for controllers could be applied to processors as well. More often than not, the core activities of the processors are determined to a large extent by the core activities of the controllers. Consequently, processors may be required to appoint a DPO whenever their controllers have a duty to appoint DPO. Where a processor carries out activities for controllers whose processing requires a DPO, and at the same time carries out activities for controllers whose processing does not require a DPO, the processor should only be obliged to appoint a DPO for the processing which falls within the remit of article 37(1). The processor may of course voluntarily choose to appoint a DPO to oversee its processing for all its clients as a matter of best practice.

- In CIPL's view, in practice, it may be the case that controllers may contractually require their processors to appoint a DPO unless the processor already has a DPO. This may happen for various reasons including the controller's GDPR obligation to appoint a DPO, best practice or industry standard.

[21] Recital 97, GDPR and [●].

c. Where the core activities" of controllers and processors "consist of processing on a "large scale" of sensitive personal data[22] or personal data relating to criminal convictions and offences[23]

The points raised in b. on the **"regular-systematic-large-scale" test** also apply to this ground. Consequently, in many cases, companies processing large-scale sensitive personal data and criminal convictions/offences data would not have to appoint DPOs as long as these operations do not constitute their "core" activities. The "core activities" of companies can only be determined on a case-by-case basis.

For example, pharmaceutical companies, insurance companies, healthcare providers and charities are likely to process sensitive personal data as part of their core activities and are likely to be required to appoint DPOs. However, it might be interesting to examine in the case of pharmaceutical companies, where the data might be pseudonymised or anonymised, whether such data might not be subject to all GDPR protections in the same way as non-pseudonymised personal data would be and, therefore, a DPO may not be warranted. Further, it appears that companies providing background checks as their core service would also have a duty to appoint a DPO. Generally, however, some private sector organisations may process criminal convictions and offences data as ancillary rather than "core activities." Relatedly, this provision should not apply when companies investigate the background of their potential vendors or when employers routinely conduct background checks before or during employment in accordance with the applicable employment and data privacy laws.

d. Where mandated by Member States' law.

This "open clause" may lead to **national inconsistencies** about the appointment of mandatory DPOs and hinder the uniform implementation and enforcement of the GDPR across the EU. It is likely that countries that already mandate the appointment of a DPO will continue to do so. Ultimately, this may be confusing for individuals who are exercising their GDPR rights across the EU or simply seeking a point of contact with an organisation, particularly where they may be more than one person listed as the DPO, one fulfilling the GDPR requirements, and one fulfilling differing national requirements. For example, a global or pan-European company may appoint a global DPO or an EU DPO to comply with its GDPR obligations but can still have a dedicated person with the title of the DPO to comply with national laws (e.g. Germany). European member states wishing to keep their current national requirements for a DPO should be encouraged to harmonise these requirements with the GDPR as far as possible. A company appointing a global DPO or an EU DPO should be able to have that person and their team also serve to meet country-specific DPO obligations. This would also enable a more consistent application of the company-wide data privacy program and avoid potential disagreements and conflicts between the country and group/global/ EU DPOs. It would also be helpful for smaller companies, non-profits and NGOs that have limited resources.

In CIPL's view, it is desirable to drive any inconsistences to a minimum in the spirit of harmonisation, protection of the fundamental rights and freedoms of individuals and the functioning of the internal single market.

[22] Art. 9, GDPR.
[23] Art. 37(1)(c), GDPR. Also Art. 10, GDPR.

2.2 Voluntary DPOs

Organisations which do not meet the requirements set out in Section 2.1 are not legally required to appoint a DPO but may do so under Article 37(4). However, in our view, in order to discharge their obligations under GDPR, including implementing accountable and effective data privacy compliance programmes, organisations will have to allocate responsibility for their data privacy and GDPR compliance to one or more dedicated employees (who may not necessarily have the DPO title). 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 his or her responsibilities but is not appointed as a "mandatory" DPO under the GDPR.

In many cases, as a matter of best practice, it may be appropriate for such companies to appoint **voluntary DPOs**. In particular, processors may find it easier to comply with and demonstrate their compliance with the GDPR by appointing voluntary DPOs. Appointing voluntary DPOs has numerous advantages including:

a. protecting the fundamental rights and freedoms of individuals;

b. signalling to the public and its customers that the company takes its data protection and accountability obligations seriously;

c. building, implementing and overseeing effective data protection and accountability programmes; and

d. a potential mitigating factor (when the DPO role is properly executed) when considering the appropriate sanction for a breach of GDPR.[24]

However, it is unclear whether voluntary DPOs will be treated in the same way as mandatory DPOs. For example, would voluntary DPOs have the same tasks and obligations as mandatory DPOs? Would the GDPR requirements of independence and protected employment status apply to voluntary DPOs?[25] Would companies appointing voluntary DPOs have to comply with GDPR DPO obligations, such as the adequate resourcing obligation?[26] Finally, would the same requirements of the GDPR apply to a mandatory DPO who also acts as a "voluntary" DPO in respect of all the other processing within the organisation that is not within the criteria for obligatory appointment of a DPO, discussed in section 2.1 above?

CIPL recommends that **"voluntary" DPOs** should not be subject to the GDPR's DPO requirements. Imposing the GDPR DPO requirements on non-mandatory DPO is likely to hinder the appointment of such DPOs as "best practice", especially in small and medium sized enterprises ("SMEs"). Also, the GDPR would have explicitly provided that the GDPR DPO requirements should apply to non-mandatory DPO if this was intended by the legislators.

[24] Article 83(2)(c), GDPR.
[25] See Sections 3.3 and 5.1.
[26] See Section 6 below.

Equally, to ensure flexibility for all different types and sizes of organisations, a remit of a mandatory DPO under the GDPR could be limited to the specific processing covered under GDPR's DPO appointment criteria, allowing the organisation to manage data protection compliance by appropriate teams.

2.3 Group DPO – Expertise and Location

Just like public bodies and authorities can appoint a single DPO, the GDPR also provides that a group of undertakings can appoint a **single DPO for the group**, provided that the DPO is easily accessible from each establishment.[27] This is a welcome approach and reflects the current practice by many multinational organisations that already appoint a European or global DPO to oversee all their entities. Group DPOs often ensure that the entire corporate group develops and implements consistent data privacy programmes, policies and practices, including internal governance, infrastructure and training and communication. In large enterprises a group DPO also is far more likely to be sufficiently senior, as envisioned by the GDPR.

However, the GDPR **group DPO provision** raises the following three key **challenges** that require further guidance.

a. It may be tricky for a single group DPO to develop and maintain **"expert knowledge"** of all the relevant European data protection laws – a key appointment requirement – especially considering the potential national divergences (e.g., national implementation of the GDPR's "open clauses" as well as national employment and freedom of expression laws). One potential way forward would be to recognise that a group DPO can benefit from the local assistance and data protection knowledge of the relevant staff in the various companies that are part of the group or from external local advisors. The data protection knowledge of the local legal teams in the various group members could be imputed to the group DPO in order to enable him or her to meet the "expert knowledge" requirement.

b. The GDPR does not specify in which country the group DPO should be **located**. In which jurisdiction should the group DPO of a multinational with a pan-European presence be located? Would such DPOs be required to be located in the same jurisdiction as their lead EU DPA? Or would such DPOs be permitted to be located elsewhere either within or outside of the EU? In our view and given the current practices of organisations with group DPOs and even CPOs outside Europe (in Asia, US or Canada), group DPOs can be located outside the EU and do not necessarily need to be located in the country of their lead EU DPA. Organisations should be able to appoint the officer who possesses the required expertise, skills and abilities required of the DPO role irrespective of the geographical location of the best candidate for this position.

c. The appointment of the group DPO raises questions about the impact (if any) of **linguistic and cultural differences** between the DPO, the "data subjects" and EU DPAs. In particular, as DPOs play important roles in ensuring that the fundamental rights and freedoms of the data subjects are protected, it is crucial that a data subject located in one jurisdiction is not hindered from contacting the group DPO located in another jurisdiction in order to exercise his or her GDPR rights and raise issues connected to the processing of their personal data.[28] This goal can be accomplished if the

[27] Art. 37(2), GDPR.
[28] See Section 7.

Group DPO is empowered to handle matters using local and other team members and resources, as well as external local advisors, who have needed language capabilities, for example.

3. The "Personhood", Liability and Employment Status of DPOs

3.1 The "Personhood" of DPOs

The GDPR DPO provisions do not specify whether a DPO can be a "natural" or a "legal" person, notwithstanding the fact that the text refers to "his or her expert knowledge"[29] and "he or she"[30] on various occasions. However, by providing that the DPO can be either an internal employee or external contractor,[31] the GDPR implies that the DPO can be a "legal person".[32]

If the DPO can be a "legal" person, then professional companies, such as law or consultancy firms, could act as DPOs with a dedicated member of staff or a point of contact for the organisation. This raises questions about the professional liability of such firms and the likely impact on their professional indemnity coverage. This possible interpretation also raises conflict issues, as law firms and similar organisations will not be able to act as DPOs for organisations that compete with them or have a pre-existing business relationship with them.

3.2 The Liability of DPOs

Irrespective of the "personhood" of DPOs, the GDPR is silent on whether individuals or professional firms acting as DPO can be subject to criminal, administrative and corporate liabilities.[33] In other compliance areas, such as competition, anti-corruption and export control laws, officers which take on roles that are broadly similar to DPOs are not subject to individual liabilities of any nature, except in cases of wilful misconduct, gross negligence, or breach of company policies or applicable law, just like any other employee would be. However, such officers may be subject to the local laws, if they are designated officers or directors of the company. This may mean that DPOs may be subject to local offences, although it is unlikely that in practice the DPO would be designated as an officer or a director of a company, in the same way as the CEO and CFO would be.

In general, we do not believe that there should be personal liability of a DPO under the GDPR and Member State criminal laws, as that may dissuade many privacy practitioners from becoming a formal

[29] E.g., Article 38(2), GDPR.
[30] E.g., Article 38(3), GDPR.
[31] Article 37(6), GDPR.
[32] Note that unlike the GDPR, Regulation REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, the first EU law specifying the DPO role, specifically provides that the DPO role be given to "at least one person," suggesting both that the role may require multiple people, but also suggesting that they must be natural persons. The GDPR does not use the term "person" in this context.
[33] Criminal liability is beyond the remit of the EU. Local criminal law may apply but many companies ask their DPO to sign a transfer of liability document so that all the various liabilities which could be attached to the DPO are attached instead to the company.

DPO and may dissuade companies from appointing a voluntary DPO. Nevertheless, the issue of DPO liability would be a useful area for further exploration.

3.3 The Employment Status of DPOs

As mentioned in Section 3.1 above, article 37(6) of the GDPR provides that the DPO can be either an employee of or an external contractor to the company.

Based on the experiences of CIPL and companies with established DPOs, the **external DPO** may not be best placed to deliver on the GDPR DPO role for large multinational organisations with complex and innovative data processing. However, this is not a hard and fast rule; ultimately, whether an external DPO may be appropriate should be a company-specific determination and depends on how the organization integrates the external DPO in its business as well as the skill-level, acumen and relevant expertise of the external DPO.

Generally, the external DPO may be particularly appropriate for companies that do not have complex processing activities and/or complex corporate structures. Equally, SMEs and start-ups whose main activities do not involve large-scale, regular and systematic personal data processing operations may benefit from being able to appoint an external DPO (who may also be part time). This would ensure that they have the required level of data protection expertise and knowledge within their organisation without incurring substantial administrative and financial burdens. For example, by employing an external DPO, SMEs and start-ups only have to remunerate the DPO for his/her hours of work rather than as a full-time employee.

In our opinion, it is important to recognise that one size does not fit all. Different organisations need to preserve the necessary flexibility in implementing the requirements of GDPR for **full v. part time[34], and internal v. external DPO** as it best suits their size, complexity and specificity of processing and industry sector. Key matters they will have to address include the following.

a. For what types of companies (e.g. size, type and volume of personal data processing operations) would an external DPO be recommended? For example, it is doubtful that an external DPO can develop a sufficiently detailed knowledge of the business, its products, its operational developments and its processing activities in order to **perform effectively his/her DPO tasks** in large multinational companies with complex personal data processing operations. In this scenario, due to his or her limited involvement with the company in question, the external DPO may not always be able to fully and effectively ensure compliance with some GDPR obligations (e.g. accountability obligations, privacy by design and DPIAs).

b. Irrespective of the size and personal data processing operations of companies, it is questionable to what extent external DPOs can be **truly embedded within their organisations** and develop productive working relationships with their colleagues in order to deliver on their GDPR roles. It is

[34] On part time DPO, see Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.

even less likely that an external DPO can have a wider **data governance and strategic role** and be close to the company's data strategy. DPOs have to become a trusted business advisor in order to undertake their various DPO tasks under the GDPR, including informational, advisory and monitoring tasks.[35]

c. Organisations need to ensure that external and part-time DPOs **devote sufficient time** to their business to discharge all their GDPR functions, given that such DPOs are very likely to take on other DPO roles, that do not breach their "no-conflict" obligations, elsewhere.

d. Given that external DPOs are likely to take on other positions, this may raise **confidentiality and conflict of interest issues** for both the employing organisation and the external DPO. Companies may have to develop internal confidentiality and conflict checks policies which are binding on the external DPO and allocate resources (e.g. staff) to implement these policies over the lifetime of the service agreement.

4. Selection Criteria for DPOs: Knowledge, Professional Qualities and Abilities

Article 37(5) of the GDPR provides that DPOs should be appointed on the basis of their "…professional qualities and, in particular expert knowledge of data protection law and practices" and the ability to undertake the DPO tasks.[36]The GDPR does not specify the professional qualities, the level of expert data protection knowledge and abilities which DPOs should possess in order to carry out their GDPR tasks. The GDPR also does not specify whether DPOs should possess knowledge of related fields, such as information security standards.

As an initial general comment, if it is accepted that in many companies, the DPO tasks[37] will often be performed by a team of individuals headed by the DPO rather than one single person, it would be useful if the WP29 could confirm that the **"knowledge-quality-ability"** criteria would apply to the DPO staff and not just to the head, lead or 'official' DPO. This would provide more flexibility for companies to organise their privacy function in accordance with their own internal organisation and to ensure that appropriate expertise is available where it is needed. It is unlikely that one single individual will have all the knowledge, professional qualities and abilities required of the DPO role.

4.1 Knowledge Requirements for DPOs

The GDPR **knowledge requirement** for DPO raises **two issues**:

Firstly, the GDPR specifies that DPOs should possess "expert" **data protection law knowledge**. The GDPR further provides that companies have the onus of determining the specific level of expertise which their DPOs should possess taking into account their personal data processing operations and the data protection required by such operations.[38] This would imply that more complex or global or sector-specific organisations will need to look for a DPO who has the appropriate level of expertise for such

[35] See Section 7.
[36] [●]
[37] See Section 5.2.
[38] Recital 97.

situations or sectors. Relatedly, the GDPR does not spell out whether group DPOs should have "expert" knowledge of the data protection laws of all the EU countries in which the organisation operates.

Secondly, the GDPR does not prescribe whether DPOs should also be **experts in other related areas,** such as information security standards. Existing research and opinions from EU DPO associations and the European Data Protection Supervisor may be apposite here. For example, a study conducted by the German Association for Data Protection and Security concluded that DPOs should also have sound knowledge of information security standards in order to discharge their DPO duties effectively. The European Data Protection Supervisor considers that DPOs should have a detailed knowledge of their companies as well as "good working knowledge" of the relevant data protection laws in order to undertake their tasks effectively.[39]

CIPL makes the following recommendations and observations on the knowledge requirements for DPOs.

a. It is questionable to what extent it is realistic to expect that every **DPO develops and maintains in-depth knowledge** of the data protection laws and practices of various European and even global jurisdictions. While this may be possible for experienced and long-standing DPOs, such DPOs may be rare to find. Data protection laws can be very complex and distinct when taking into account national divergences in terms of the implementation of the GDPR "open clauses", local data practices (e.g. the distinct approaches of EU DPAs and the cultural expectations of local data subjects), the interactions between national data protection laws and other national laws (e.g. consumer protection, banking, insurance, e-commerce, labour, anti-money laundering or criminal laws) and multi-sectorial clients in case of processors.

b. A possible way forward would be to enable the DPO to have access to **the local internal staff or external advisors** who have up-to-date knowledge of the relevant data protection laws and practices. This reflects the current practices of other corporate compliance, in-house legal and the General Counsel roles. This could be done pursuant to the adequate resourcing obligation of companies pursuant to Article 38(2).[40] As mentioned earlier, and a point worth repeating, the expertise in and knowledge of local data protection laws by the staff or external advisors of the DPO could be imputed to the DPO to enable him or her to meet the GDPR "expertise" requirement under the GDPR. It is perfectly acceptable and customary for DPOs to seek frequent legal, consultancy and technical advice from external consultancies and law firms. This practice is likely to continue after the GDPR becomes applicable especially taking into account the increased legal and operational complexities introduced by the GDPR. It is also common and best practice for DPOs to work closely with internal experts in other areas, such as information security, HR, marketing and so on to get to compliant solutions and to implement legal and policy requirements.

c. Some **specifics** are best left to organisations and their HR departments when looking for the right candidate for the DPO role. For example, the level of expert knowledge and the years of practical experience in the relevant fields a DPO should have to qualify as an "expert". The relevant expertise level required by a DPO will vary from organisation to organisation and will

[39] EDPS opinion, pp 9 **[Which EDPS opinion? Need to find]**
[40] GDPR. See Section 6.2.

depend on several factors, including the volume and nature of data processing operations of companies, the types of personal data processed and the data protection issues raised by these processing operations and personal data types.

d. Organisations may want to assess the percentage of the DPO's tasks that would require legal background or knowledge. This may vary between different companies depending on the nature of the company and its data processing operations. For example, IT service and outsourcing providers may need a DPO or someone within their DPO team with a legal background if one of the main tasks of their DPO would involve reviewing and negotiating data privacy terms in client contracts.

e. The advisory tasks of DPOs could require legal knowledge and experience. Hence, some companies may find it preferable to appoint someone with a legal background and legal experience to save costs of having to constantly refer legal issues to others internally or externally. However, the DPO role also has many other non-legal aspects and we do not believe that a DPO role should necessarily always be a legal role. As mentioned earlier in this paper, the DPO is not necessarily one single officer. Indeed, in many cases it will be hard to find a single person who has all the necessary knowledge and skills required for the role (e.g. legal, operational, project management, strategic, technical and external representation). In such cases, it is important that DPOs have the appropriate support of a DPO team.

4.2 Professional Qualities and Abilities of DPOs

The GDPR does not expand on the professional qualities and abilities which DPOs should possess so that they can discharge their GDPR roles effectively. In our experience, an effective DPO will require the following skills.

a. **Interpersonal and communication skills**: DPOs have to be able to communicate, negotiate, resolve conflicts and build fruitful relationships with various external and internal stakeholders (e.g. EU DPAs, individuals, management of the company, the different company functions, civil society and advocacy groups) and across various cultures and jurisdictions.

b. **Organisational and privacy program management skills**: DPOs need advanced organisational skills so that they can carry out all their tasks and be able to build, implement and oversee the privacy programmes of their organisations effectively.

c. **Leadership skills**: DPOs require advanced leadership skills so that they can drive data privacy compliance within their organisations and manage a team of DPOs or privacy advisors. DPOs who operate within a team should be capable of delegating tasks as well as guiding, instructing and overseeing their team.

d. **Data privacy strategy skills**: DPOs are more than just compliance officers. Their role includes setting the data privacy strategy for their organisations and linking that strategy to business imperatives and organisational culture and drivers.

e. **Business skills**: The DPO may also perform the role of a chief data strategist and be a business enabler for data driven innovation, while protecting the fundamental rights and freedoms of individuals. As such, the DPO must have a strong business acumen, a firm understanding of the

corporate data strategy and the relevance of data privacy compliance for data and business strategy.[41]

f. **Technology skills:** DPOs should have a solid grasp of the technologies implicated in the processing operations they oversee, as well as of the processing operations themselves.

5. DPOs: Independence, Organisational Position and Confidentiality Duties

5.1 Independence of DPOs

Several GDPR provisions emphasise the "independent" status of DPOs. Article 38(3) of the GDPR provides that the DPOs should not receive any instructions from their employers or contractors regarding their DPO tasks. Article 38(3) also provides DPOs with a protected employment status. This means that organisations cannot dismiss or sanction DPOs for performing their DPO tasks. Recital 97 adds that DPOs ". . . should be in a position to perform their duties and tasks in an independent manner." However, the "independence" of DPOs is not absolute. The DPO is an employee of the company and the DPO is required to report to the "highest management level" of their organisation.[42] In some ways this is a further confirmation of the operational independence and the DPO's accountability to most senior management.

As analysed next, the GDPR provisions on DPO independence raise three issues which require further consideration, namely, (1) the meaning of independence, (2) the practical difficulties of establishing direct reporting lines with the "highest level of management" in global organisations and (3) the practical difficulties raised by the protected employment status of DPOs.

5.1.1 DPO Independence: Operational or Full Independence?

There are two possible ways in which the GDPR provisions on the **independence of the DPOs** can be interpreted. The first possible interpretation is that DPOs should be operationally independent so that they can undertake their DPO tasks whilst not being totally independent from senior management which sets out the strategy of their organisations. From this perspective, DPOs will have to discharge their GDPR functions in a way which is consistent with such strategies.

The second possible (and more problematic) interpretation is that the DPOs are positioned as being fully independent from their organisations and acting as "mini-DPAs" or "policemen" within such companies. If this interpretation is adopted, there is a danger that the DPOs will not be fully integrated into and involved by their organisations. This may result in DPOs being viewed internally with a degree of suspicion. In this scenario, other employees may distance themselves from the DPOs. They may view the

[41] The DPO role might be analogous in many ways to the role of the CFO, which carries both operational and strategic responsibilities to customers and the CEO or Board. A CFO is responsible for delivering operational growth of a company through its financial accounting team and its strategic responsibilities through its financial management team, with ultimate responsibility for both lying with the CEO. A CFO also engages with and is responsible for the company's relationship with its regulator, engaging with said regulator at various points to discuss the company's overall strategy, potential pipeline of products, etc., and also to engage directly in the event of a financial issue directly affecting customers and shaping regulatory thinking and guidance.

[42] Art. 38(3), GDPR.

DPO as a police officer rather than as a trusted business advisor or a problem solver. This isolation would prevent DPOs from being able to perform their GDPR roles effectively.

For example, if employees of an organisation do not consider the DPO as a trusted team member, they may have qualms about involving the DPO in new projects from an early stage. This would prevent the DPO from adding value at the very outset by embedding data privacy advice and compliance measures in the early design stages of the project. For many organisations, early DPO involvement in new projects has several benefits including improving data privacy compliance, enhancing the protection of the fundamental rights and freedoms of individuals, and treating data privacy as a value-add. Otherwise there is a risk of privacy being considered as requiring simply a legal minimum. If we consider the experience of organisations with comprehensive and mature data privacy compliance programmes, it is evident that in many cases the most effective corporate privacy management programmes are 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 police officer or legal check box.[43]

Thus, similar to the first option presented above, a common-sense approach might be to recognize that since a DPO works within an organization, he or she cannot be completely independent by definition, but that he or she also must have an appropriate degree of operational independence consistent with the relevant GDPR DPO requirements, particularly Article 38(3). Accordingly, while there may be an "enforcement" element to the DPO role, the task will be to operationalize it in a way that benefits the organization while also furthering the goals of the GDPR. A list of "best practices" to implement this approach may be useful.

5.1.2 Global Companies and Direct Reporting Lines of DPOs

It is not clear what the GDPR means by the **"highest management level"**, in particular in the context of group DPOs in global companies. Does the "highest management level" refer to the Chief Executive Officer ("CEO"), the Management Committee or the full Board? Is it the local management in the country of DPO, at the EU level or at global level?

We believe that reporting lines should be "true" reporting lines to the management that has the authority to, for example, make binding decisions, effectuate real change or adapt a privacy program after a specific incident or non-compliance issue. For example, an EU DPO should not have to report to an EU MD/CEO where the appropriate management line that has the relevant strategic influence within the company is located in the parent company based outside the EU. In such cases, artificial reporting to an EU MD/CEO would undermine the aims of the GDPR.

The relevant reporting lines may also vary depending on the company or the reported issue. One specific issue may require a direct reporting line to a specific manager whilst another may require a different direct reporting line to another manager. Organisations need to have the flexibility to determine the most appropriate reporting line for DPOs and enable DPOs to "have a seat at the table" and collaborate with a wider group of highest management.

[43] CIPL (2015), *supra*, note 14.

Companies should also have the flexibility to determine the best way to operationalise the reporting requirement taking into account the specific context of their organisations and the tasks of their DPOs. For example, a direct report to a member of the Management Committee or the CEO may only be necessary where there is a conflict. Another example of operationalizing the reporting requirement is that it could be met by periodic DPO reports given to a CEO or to a Board committee even if the DPO for employment purposes reports to someone else who is not the CEO. In the absence of a specific conflict, other "reporting" or communication lines might be more effective. Further, some DPO tasks that are not strictly within the statutory DPO responsibilities could follow a different reporting line. This flexibility in establishing effective governance as it relates to reporting should be approved at that highest level of management.

Moreover, multinational companies that currently appoint central DPOs/CPOs outside of the EU will have to pay particular attention to the GDPR DPO provisions on direct reporting lines. In particular, many multinational companies may find that under their current organisational framework, DPOs that are based in Europe may not yet have direct reporting lines to the "highest management level" which may be located in various non-European jurisdictions. Equally, some EU DPOs currently report to global CPOs who may be located anywhere in the world and may not be the "highest management level". As mentioned, this is entirely appropriate as it helps to ensure that there is a global approach and strategy to corporate data privacy and compliance programs. Local EU DPOs who are members of a global DPO/CPO team should still be able to report to a global DPO/CPO, if that DPO/CPO reports to the "highest management level". The same applies to DPOs who report to a C-suite officer, such as the General Counsel, and it is important to bear in mind that in some organizations both the global DPO/CPO or General Counsel may be outside of the EU

[May add diagram with mock reporting lines in next version]

A final question is whether the CEO can designate a member of his or her executive team to oversee routine DPO reports especially in large or multinational companies where the CEO may not personally be able to handle all DPO issues. We believe that the answer to this has to be in the affirmative, particularly in large companies. It is unrealistic to expect a CEO of a multinational company, for example, to be the direct reporting line of an EU DPO. For most companies, a DPO reporting to this level will not have full or even part-time responsibility, nor the necessary knowledge of data privacy and would not be able to effectively implement GDPR. In these circumstances, there is usually a senior leadership team / Management Committee that reports to the CEO. Data protection responsibility may often be within the remit of such teams. Consequently, depending on the circumstances, it may be more appropriate for an EU DPO to report to such teams as they are responsible for the global regulatory compliance (including data protection) of their organisations.

5.1.3 Protected Employment Status of DPOs

The **protected employment status of DPOs** pursuant to Article 38(3), has several advantages including protecting DPOs in situations where their data privacy assessments contradict the business interests of their employers. This provision and the "independent" status provision provide DPOs with the reassurance that there will be no retaliation when they perform their GDPR tasks, thus, enabling DPOs to perform their role fully.

However, this provision may also present a number of practical difficulties for organisations, especially in the context of internal performance management and review processes. Values and criteria for good performance will differ from one organisation to another and may conflict with what the EU DPAs and the GDPR expect from DPOs. As an example, a DPO who prevents a new product or service from being launched based on data privacy compliance objections might be deemed a poor performer by his/her employers although s/he may have met his/her GDPR DPO obligations. Or, what if the DPO takes a very narrow (but justifiable) approach to "legitimate interest" based processing, thereby hindering certain benefits to the company, individuals and society? Can the company leadership sanction or terminate the DPO? Presumably not, based on Article 38(3) (does not "receive any instructions" regarding the DPO tasks; "shall not be dismissed or penalized").

Furthermore, and importantly, in terms of resolving performance issues, such as poor performance and gross misconduct and other behaviours that are not related to the specific statutory DPO tasks, there is a risk that these issues may be conflated with the "protected employment status" of DPOs rather than handled separately as employee performance issues. An organisation should be able to maintain appropriate performance standards and review processes over its employees, including its DPO and DPO staff. There may be scope for further guidance on situations where performance evaluations touch on substantive deficiencies in relation to interpreting and applying the GDPR.

Finally, it must be taken into account that if the protected employment status is taken to its extreme, or becomes similar to the protected status of Works Councils employees in some EU countries, this may dissuade organisations from appointing internal DPOs. They may instead opt to appoint external DPOs whose roles are much more flexible and whose contracts can easily be terminated.

5.2 The Organisational Position of DPOs

Further WP29 guidance should clearly establish whether the GDPR DPO requirements may be met by a **single DPO** and an **entire DPO office** with a "lead" DPO and DPO staff. In many cases, it may be highly unrealistic to expect one single person to undertake all the DPO tasks, taking into account the:

a. size of the organisation;

b. pan-European or global presence of companies;

c. nature, scope and risk of their personal data processing operations; and

d. expertise level required for such types of companies and processing operations.

In such cases, the DPO will require the assistance of a team of specialised experts including perhaps a deputy to enable him or her to discharge his or her role effectively. This approach will also enable DPOs to meet their "expertise" requirement under the GDPR.[44] This course of action is in line with standard practice by many DPOs who seek legal and other expert advice both from within and from outside counsel and other advisors. In our experience, such standard practice will continue.

[44] Section 4.1.

Consequently, it may be more appropriate to interpret the GDPR concept of the DPO as including not just an individual officer but also an **entire DPO office**, with staff encompassing multiple specific roles, requirements, locations and skills, which is headed by a "lead" DPO. CIPL believes that this interpretation of the notion of the "DPO" is essential to enable multinational companies to meet their GDPR DPO obligations. This position is also consistent with and follows from Article 38(3) to the extent the DPO must be provided with the necessary resources to carry out his or her tasks.

This suggestion is in accordance with the practices developed by European institutions which have appointed DPOs for several years. For example, some European institutions have appointed a head and assistant DPO whilst the European Commission has appointed a "data protection co-ordinator" in each Directorate General ("DG") to co-ordinate all aspects of data protection in the DG in question.[45] The European Commission used this approach because of the size of the institution and the importance of having local support at the DG level. Drawing from these practices, it is clear that where appropriate, a DPO can denote a department with a head and deputy DPO as well as staff members. [46]

5.3 DPO Duties of Secrecy or Confidentiality

Article 38(5) provides that DPOs are bound by **secrecy or confidentiality obligations** when performing their GDPR tasks in accordance with European or Member State laws.[47] The GDPR grants Member States the discretion to introduce national laws on the duty of confidentiality or secrecy of DPO which may lead to the further fragmentation of the DPO requirements at the EU level. In addition, taking into account that a DPO role may be exercised by a lawyer, including an external lawyer, some clarification will be required regarding the legal privilege pertaining to the DPO tasks and its interaction with any duty of confidentiality.

We are also concerned that the confidentiality duty towards the organisation that employs the DPO may conflict with the DPO's reporting duties and their ability to effectively perform their DPO role. Indeed, this requirement may be hard if not impossible to apply in absolute terms within the organisation. The DPO must be transparent to the organisation that retains or employs him or her. Indeed, to be effective, a DPO cannot be a "silo" and operate shrouded in veil of secrecy. A broad interpretation of what kind of information must be kept confidential and vis-à-vis whom may conflict with the DPO's legally enforceable employee duties or duties of loyalty. It should also be clarified how this duty interacts with the reporting requirement to the highest management level and whether these reports are not covered by the duties of secrecy and confidentiality. In short, given that DPOs are (and should) be integrated within their organisation, it is difficult to see how this provision can be fully applied towards the company employing the DPO. The company's leadership and other relevant management need to know and be involved in any contentious and serious data privacy compliance issue.

---

[45] [●].

[46] Another example at EU level is Europol that has a data protection office with several staff, headed by the DPO.

[47] Some European member states already have similar provisions. For example, the German DPA responsible for the private sector states that that the independence of the DPO could be ensured, for example, by having "DPOs […] bound to confidentiality about the identity of the data subjects, as well as the circumstances under which they obtained information about a data subject, unless otherwise specifically authorised by the data subject in question." [●] In Netherlands, the Data Protection Act provides that when the DPO carries out an investigation into sensitive areas, such as concrete security arrangements or matters involving sensitive data, such information must be kept under utmost confidentiality. [●]

We propose that this obligation is interpreted to mean the following.

a. The DPO has a limited duty of confidentiality and secrecy vis-à-vis the company in respect of contentious personal data matters and data breaches. This duty could be discharged on a "need to know" basis which is appropriate to the context.

b. The DPO has a duty of confidentiality and secrecy towards any third party as set out in the confidentiality provisions of the DPO's employment contract.

6. Duties of Organisations towards the DPO

6.1 Proper and Timely DPO Involvement

Article 38(1) of the GDPR requires organisations to involve the DPO **"properly and in a timely manner"** in all data protection issues.

This provision aims to ensure that the DPO can proactively execute his or her GDPR tasks for the benefit of the organisation, individuals and the relevant EU DPAs. The terms "properly" and "timely" indicate that organisations must enable DPO involvement in a manner and at a time that is useful and effective depending on the relevant circumstances. Furthermore, this provision also suggests that the burden is on the companies to involve the DPO in all data protection issues.

However, in practice, it may not always be apparent to the employees of a company that data protection issues are raised by an initiative. Thus, organisations should establish appropriate processes as part of their accountability and compliance programs (and in particular the privacy-by-design principle) to ensure the appropriate and timely involvement by the DPO and the DPO's staff. Specifically, we recommend that organisations establish internal processes relating to DPO involvement to facilitate appropriate decision-making about this matter at all levels. For example, internal project teams may be required to subject their initiatives to a data protection pre-screening process to assist them in evaluating whether data protection issues are raised. This is well-known "best practice" used by many companies. This pre-screening process might also consider the level of risk to individuals that may be associated with the initiative to enable prioritisation of DPO involvement.

6.2 Access to resources

Article 38(2) provides that companies have the **obligation to "support" DPOs** when they perform their DPO tasks[48] by providing DPOs with:

a. the resources necessary to carry out these tasks;

b. access to the relevant personal data and processing operations; and

c. the resources necessary to maintain their expert knowledge.

[48] See Section 7.

This is an important provision which recognises that effective data privacy accountability and compliance by DPOs can only be achieved when they are adequately resourced. Depending on the ultimate application of this Article, it may also be important in light of the fact that Article 83(4)(a) makes an infringement of this provision subject to the GDPR's significant fines of up to 2% of an organization's total worldwide annual turnover. Further considerations and recommendations concerning this provision include the following.

- In terms of "resources", this provision could cover resources such as compliance technology and tools, IT resources, staffing resources, access to external legal, technical and consultancy advisors, and an adequate and separate budget for DPO activities and staff. As argued earlier, in many cases, it will be unrealistic to expect one single DPO to be able to deliver all the DPO tasks. Consequently, in practice, DPOs will need to have sufficient resources in terms of access to staff or appropriate teams to ensure that they can discharge all their tasks effectively. For example, DPOs will need access to staff to respond to and deal with internal and external queries, complaints and requests for exercise of data rights expeditiously and effectively. As another example, global DPOs will need access to local staff members or external legal counsel, who have up-to-date knowledge of the national data protection laws and practices.

- It appears that organisations will need to provide adequate resources for the DPOs to "maintain" their expert knowledge on an ongoing basis. This must apply to the entire DPO staff. As data privacy laws and technologies evolve rapidly, it is essential that DPOs and their staff have an up-to-date knowledge of the relevant fields so that they can carry out their DPO tasks effectively. Relevant DPO knowledge includes data privacy laws, business models, compliance, best practices, accountability and data protection compliance tools and technologies, IT and sector-specific knowledge where appropriate. This can be provided on a continuous basis, just like with continuing professional education requirements for lawyers or other professions. Given the proliferation of professional privacy and security certifications, it is likely that these types of certifications may also be appropriate to provide continuous education to DPOs and their staff.

- Should there be a single preferred certification and training for DPOs, or is pluralism and competition useful here? We can imagine that several well-established certification schemes can serve as acceptable training for DPOs. However, we can also envisage further professionalisation of training and certifications by relevant professional associations (e.g. IAPP and others). This may include courses delivered in conjunction with higher education institutions. Certification and training are best left to market forces rather than be subject to any edict from EU DPAs.

- A subject worthy of further consideration might be the content of the GDPR DPO certification courses. For example, such courses should cover not only data protection law and practice, but should cover other subjects, such as relevant IT knowledge and DPO-specific skills.

- What steps can be taken to ensure that companies, such as start-ups, can secure the relevant funding for training their DPOs during their funding rounds? For example, it may be important to educate investors to make them aware of the necessity of initial and ongoing data protection training for DPOs so that they do not reject such items outright when they consider the financial models presented by start-ups during funding rounds.

- Suitable guidance needs to be provided by the WP29 to SMEs and start-ups on how they can meet their "resources" obligation under the GDPR.

- Given the inherent difficulty in establishing clear *ex ante* guidelines on what constitutes adequate levels of support of the DPO function under this GDPR requirement, we recommend that any such adequacy only be evaluated on a case-by-case basis in conjunction with the evaluation of other alleged substantive violations which may be attributable to the lack of adequate support. In other words, we do not recommend that in many cases the inadequacy of support be treated, evaluated and penalized as a stand-alone violation.

6.3 Conflict of Interests

The GDPR does not preclude the DPO from fulfilling non-DPO tasks and duties. However, the employer of the DPO has a duty to ensure that these non-DPO tasks and duties do not result in a **conflict of interest**.[49] Conflicts of interest may also arise when the DPO task of consulting with the EU DPAs is interpreted broadly to mean reporting to the EU DPAs on the details and issues relating to a company's compliance program. In addition, this provision raises the following issues.

a. Which roles within the organisation may be compatible with the DPO role? The Düsseldorfer Kreis, which has provided guidance on the role of the DPO under German law (and which is not shared in other EU jurisdictions), has identified a number of roles, such as the Human Resource and Information Technology Director that are incompatible with the role of the DPO.[50] Equally, the Chief Marketing Officer and Chief Information Security Officer roles may be incompatible with the DPO role, as both roles may require uses and processing of data that may create data privacy compliance issues. Further, is the role of "chief data strategist" compatible with the DPO role? The potential conflict raised by the roles of DPOs as chief data strategists and compliance officers may be different with respect to external DPOs who are also advising other organisations.

b. Our experience shows that some Chief Privacy Officers combine their roles successfully with the roles of information governance and chief data strategist. Indeed, we believe it is the very essence of a strategic DPO role to combine compliance functions and fundamental rights protection, with the roles of business enabler and data strategist. It is only the DPO that will have the knowledge and skills to be able to balance these various interests whilst protecting the fundamental rights and freedoms of the individuals. The truly successful and effective DPOs should be able to maximise the effectiveness of each of these roles without experiencing or creating conflicts. This is the only way in which the DPO can become more strategic, more senior and have a wider data governance role, as opposed to a simple legal compliance role.

c. Should this provision be interpreted strictly as preventing external DPOs from taking on DPO roles in other companies? This will be of relevance to external and part-time DPOs which will often be used by companies with limited financial resources, such as some SMEs and start-ups. External and part-time DPOs should not be prohibited from taking up roles and positions in

[49] Article 38(6), GDPR.
[50] [●].

other companies as long as such roles do not conflict with their DPO role. Such exclusivity must be remunerated and a back-up DPO could be required in case a conflict of interest arises. The contract between the DPO and the company employing the DPO may include specific provisions, such as the obligation of the DPO to notify the company before taking up new roles and the ability of the company to veto any proposed role of the DPO elsewhere in cases where there is a conflict of interest, to ensure compliance with the GPDR. This makes sense given that the GDPR places the burden of responsibility for this duty on the organisation rather than the DPO. Finally, the organisation may also benefit from introducing conflict checks procedures and policies which are triggered each time the DPO notifies the company that s/he is considering taking on a new role elsewhere.

7. Tasks of the DPO

Article 39(1) of the GDPR sets forth the following tasks of the DPO:

a. **Information**: DPOs have the obligation to make their organisations aware of their data protection obligations and responsibilities under the GDPR. This would include providing the organisation with information about their GDPR compliance obligations towards their customers and employees. It would also include training, awareness and communication activities, which should be an integral part of their data privacy program, as well as briefing leadership about the company's GDPR obligations and associated risks.

b. **Advice:** Article 39(1)(a) provides that DPOs must provide their organisations (including relevant staff members) with advice on their data protection obligations both under the GDPR and the applicable national data protection law. The advisory task is multi-faceted and depends on the processing operations of the organisation. The GDPR specifies that DPOs have to provide advice on data protection impact assessments ("DPIA")[51]. DPOs can also provide guidance on compliance and accountability measures in particular in the context of risk.[52]

c. **Monitoring**: DPOs have to monitor the compliance of the organisation with the GDPR, applicable national data protection laws and its own internal and external data protection and security policies. Article 39(1)(b) provides the following non-exhaustive list of matters which DPOs should monitor, namely, assignment of data protection responsibilities, data protection awareness initiatives and training sessions of the staff involved in personal data processing and related audits.[53] DPOs also have the obligation to monitor how DPIAs are performed.[54]

d. **Co-operation with DPAs:** DPOs have an obligation to co-operate with the EU DPAs.[55] This task emphasises that the GDPR envisages that DPOs will provide crucial links between their organisations and EU DPAs in several contexts, including investigations, complaint handling and prior consultation, but also more generally in the context of demonstrating organisational accountability on request by DPAs. DPOs will be expected to have detailed knowledge of their

[51] Article 39(1)(c), GDPR
[52] Recital 77, GDPR.
[53] Article 39(1)(b) , GDPR
[54] Article 39(1)(c), GDPR.
[55] Article 39(1)(d), GDPR

organisation's processing operations and business drivers and be able to communicate those to DPAs on request and as appropriate.

As part of this co-operative function, the DPOs may also have to share information with EU DPAs about relevant aspects of their organisations, including the personal data processing operations; internal data protection policies and practices; risk assessment procedures; DPIAs and how their organisations meet their GDPR accountability obligations. The volume and types of information which the DPOs will have to share with EU DPAs will depend on the tasks conducted by the EU DPAs at that point in time (e.g. complaint handling, investigation). It is more likely that the co-operative task will be triggered once the EU DPA reaches out to the DPO to obtain further information about a specific matter (e.g. complaint filed by an individual).

However, the issue of co-operation with EU DPAs as well as complaint handling for individuals must be further considered in light of the fact that most corporate legal departments would not want their DPOs communicating and providing information directly to an EU DPA. The DPOs may also be bound by a legal privilege obligation. Some companies may require their DPOs to involve their in-house or external legal counsel in communications with or about complainants. In addition, if the DPO is also an in-house data protection counsel, the DPO may be precluded from sharing information with the EU DPAs under the relevant local laws that govern legal privilege. Further, given the "independence" and "reporting lines" requirement, it appears that the highest management level might have to be involved in these matters as well if there are any disagreements between the DPO and counsel. Thus, any future guidance on this subject should address these issues and recognize that the cooperation requirement under Article 39(1)(d), may be circumscribed by other relevant obligations.

e. **Consultation with EU DPAs**: DPOs have an obligation to "consult" with EU DPAs on relevant data protection matters, where appropriate.[56] It appears that the DPO's loyalty duties would not enable the DPO to make such consultation with EU DPAs without informing the company. This is currently the case for consultations with regulators in other sectors (e.g. financial or competition regulators). It is also unclear whether the communications between DPOs and the EU DPAs are confidential.

We do not believe that this obligation should be interpreted to mean that the DPOs should report breaches and non-compliances to EU DPAs outside of the formal company breach notification policy and process. It is likely the DPO will be the contact point for the EU DPAs where breaches are formally reported. Further WP 29 guidance on when and how such consultations should take place would be useful to outline how to implement this obligation without undermining the role of strategic and trusted business advisor and ultimately the DPO's effectiveness and credibility within the organisation.

Finally, the consultation obligation again raises the issue of how corporate counsel will be involved in any communications with the EU DPAs, especially in countries where in-house counsel communications are protected by legal privilege. Thus, as with the obligation to cooperate, any guidance on the issue of consultation should consider the possible impacts of parallel or conflicting obligations of the DPO.

[56] Article 39(1)(e),GDPR

f. **Contact Point for EU DPAs**: DPOs have the obligation to act as the point of contact for EU DPAs on personal data processing issues including prior consultation.[57]

g. **Contact Point for "Data Subjects"**: "Data subjects"[58] may elect to contact the DPO on all issues related to the processing of their personal data. Data subjects may also exercise their GDPR rights, such as access, rectification, erasure, objection and portability, by contacting the DPO.[59] 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. Being the contact point for the individual does not mean that the DPO is also the representative of the individual vis-a -vis the company. It is important to ensure that the external aspects of the DPO role do not interfere with or replace other established channels of communications and points of contact between companies and their customers (e.g. customer support, customer hotlines, customer complaint departments and call centres).

The GDPR implies that the DPO will have to deal with individuals' complaints and disputes. This may reduce the number of claims referred to the relevant EU DPA as individuals attempt to resolve their problems by raising the matter with the DPO. The individuals' recourse to the DPO does not affect their rights to refer their complaints to the relevant EU DPA or courts. However, to the extent the DPO is a contact point for individuals to complain, this again raises an issue about how existing complaint mechanisms function, and how in-house and outside counsel are involved, given that the complaints could relate to law violations. Whether and how to involve counsel in such interactions should be left to the individual organizations.

Member states may prescribe **additional DPO tasks** under their national laws, which may result in inconsistent DPO obligations across the EU. In our experience, further specification of DPO tasks by Member States should be avoided and any further specification of the role should be left to the organisations. In addition, further tasks can be included in binding corporate rules for the DPOs.[60] Indeed, current experience shows that the current DPO roles have an even wider remit and include more detailed data responsibilities than specified in the GDPR. This is to be expected and organisations should be free to specify the role of DPO as suits their organisation, structure and culture, consistent with the GDPR.

As an **overarching obligation** in the performance of their tasks, DPOs must have due regard to the "risk" of processing operations taking into account the nature, scope, context and purposes of processing when exercising their tasks.[61] This implies that, just like with accountability and privacy programs which can be calibrated based on risk,[62]the tasks of DPOs should be modulated in proportion to the risks to the fundamental rights and freedoms of individuals.

[57] Article 39(1)(e),GDPR
[58] Article 4(1), GDPR defines a "data subject" as an "identified or identifiable natural person".
[59] Article 38(4), GDPR. Article 37(7) requires organisation to inform the public and the relevant EU DPA of the contact details of the DPO.
[60] Art. 47(2)(h), GDPR.
[61] Art. 39(2), GDPR.
[62] E.g. Articles 25 and 28, GDPR.

8. Conclusion

The development of the role of the DPO has been a striking feature of the last decade of data protection GDPR and corporate risk management. The detailed GDPR provisions on the appointment, selection criteria, employment status, duties and tasks of the DPO provides a comprehensive starting point, but require further elaboration to implement these requirements in practice. Indeed, it raises significant practical questions as to how the role will work in practice and how it should be designed to ensure that the DPO is the strategic cornerstone of accountability and data privacy compliance whilst continuing to balance the increasingly complex interests of organisations, individuals and EU DPAs. The upcoming guidance from the WP29 on DPOs will provide a vital opportunity to clarify and expand on the role of DPOs so that such officers can discharge their roles effectively. However, such guidance should also leave as much flexibility as possible to organisations to implement the DPO role effectively as they see fit taking into account their organisational structure, culture and data privacy strategy.

Going forward, it may be in the interest of regulators to develop an incentive-based approach to both mandatory and voluntary DPOs. Relevant incentives could include the reputational benefits of appointing a DPO, linking the DPO role to accountability and delivering comprehensive data privacy programs and mitigating factors in cases of a GDPR breach. An incentive-based approach will also encourage voluntary DPO appointments for companies that may wish to minimise their compliance risk or gain the trust of their customers.

Appendix 1

OBJECTIVES OF THE CIPL GDPR PROJECT

The CIPL GDPR Project aims to establish a forum for an expert dialogue between industry representatives, EU DPAs, the European Data Protection Supervisor (EDPS), the Commission, the Member States representatives and academic experts through a series of workshops, webinars and white papers with the following specific objectives:

- Informing and advancing **constructive and forward-thinking** interpretations of key GDPR requirements;
- Facilitating **consistency in the interpretation** of the GDPR across the EU;
- Facilitating **consistency in the further implementation** of the GDPR by Member States, the Commission and EDPB;
- Examining **best practices**, as well as **challenges**, in the implementation of the key GDPR requirements;
- **Sharing industry experiences and views** to benchmark, coordinate and streamline the implementation of new compliance measures; and
- Examining how the new GDPR requirements should be interpreted and implemented to **advance the DSM and data-driven innovation**, while protecting the privacy of individuals and respecting the fundamental right to data protection.

Appendix 2

FOCUS TOPICS OF THE CIPL GDPR PROJECT
"5 BUCKETS"

1. **Data Privacy Programmatic Management**
   - Accountability and its elements under the GDPR for controllers and processors;
   - Appointment and role of the DPO;
   - Assessing risk under the GDPR – privacy impact assessments, privacy by design, breach notification;
   - Evidencing and demonstrating accountability externally;
   - Privacy seals, certifications, codes of conduct; and
   - Harmonisation and consistent implementation.

2. **Core Principles and Concepts**
   - Legitimacy (consent/age of consent, legitimate interest), decisions based on profiling, transparency, purpose limitation, pseudonymisation.

3. **Individual Rights**
   - Data portability, new aspects of data erasure and right to object, transparency.

4. **International Data Transfers**
   - Adequacy decisions, BCRs, model contracts, the new EU-US Privacy Shield, derogations, seals and certifications, Art. 48, interoperability with non-EU mechanisms.

5. **Relationship with the EU DPAs, Enforcement and Sanctions**
   - Smart regulation;
   - Main establishment, "one-stop-shop" and relationship with EU DPAs;
   - Role and powers of the EU DPAs;
   - Role and powers of the EDPB;
   - Consistency procedure;
   - Sanctions and liability; and
   - Links with EU strategy for digital single market and smart regulation.

Appendix 3

CIPL GDPR PROJECT WORK PLAN 2016

PROJECT PRIORITIES AND SUBGROUPS

WP29 and CIPL Initial Priorities

- Risk (including high-risk processing and DPIAs);
- DPO;
- E-Privacy Directive; and
- Certifications* (including seals, codes of conduct and BCRs and their roles as accountability tools and cross-border transfer mechanisms).

CIPL Midterm Priorities*

- Innovation drivers (e.g. historical/statistical research and anonymisation/pseudonymisation);
- Core principles – Consent (including the age of consent for children), legitimate interest, transparency, notice and icons; and
- Smart regulation – The roles of and relationships with EU DPAs, "one-stop-shop" and main establishment.

Each topic subgroup will develop and participate in the project activities listed below:

PROJECT ACTIVITIES

Internal	External
• Subgroups and calls • Industry project participants calls – monthly • All project participants calls – every two months • Deep-dive webinars	• Workshop reports, papers and written submissions • Ad hoc engagements with EU DPAs, European Commission and national governments • WP29 FabLab (Brussels) • Workshop II (19 September Paris TBC) • Workshop III (January 2017, Brussels TBC) • European Commission stakeholder day

PROJECT LEADS

- Bojana Bellamy, President, bbellamy@hunton.com
- Markus Heyder, Vice President and Senior Policy Counselor, mheyder@hunton.com
- Richard Thomas, Global Strategy Advisor, richard.thomas@which.net
- Dr. Asma Vranaki, Fellow, avranaki@hunton.com

**Start in Summer 2016*