Centre for Information Policy Leadership
Hunton & Williams LLP

24 January 2017

Comments by the Centre for Information Policy Leadership
on the Article 29 Data Protection Working Party's
"Guidelines on Data Protection Officers (DPOs)"
adopted on 13 December 2016

On 13 December 2016, the Article 29 Data Protection Working Party (WP29 or WP) adopted its "Guidelines on Data Protection Officers (DPOs)" (Guidelines) and associated Frequently Asked Questions (FAQs). The WP invited public comment on these documents by the end of January 2017. The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to submit the below additional brief comments. These additional comments follow up on CIPL's 17 November 2016 white paper on "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation"[1] (CIPL DPO White Paper), which CIPL had submitted to the WP29 as formal initial input to the WP's development of DPO implementation guidance under the GDPR.

As a general matter, CIPL appreciates the WP's pragmatic and restrained approach to its implementation guidance on the GDPR DPO requirements and, for the most part, supports the guidelines as drafted. In connection with the discussion of "large scale" criteria for the appointment of the DPO, CIPL agrees with the WP's assessment that it is currently impossible to provide precise guidance on all aspects of this term but that a "standard practice" may develop over time, which the WP plans to further elaborate upon in the future by way of "sharing and publicising examples of the relevant thresholds for the designation of a DPO." We suggest a similar approach to all aspects of the DPO Guidelines and that they and the other WP29 GDPR guidelines be viewed as "living documents" subject to amendment and clarification based on evolving future experience. Relatedly, we suggest that where amendments are made that change the threshold for appointing a DPO, the WP29 also provide for appropriate implementation periods to allow organisations sufficient time to come into compliance.

Further, we note that the WP29 Guidelines do not address all key DPO issues presented by the GDPR, some of which we previously addressed in our above-referenced CIPL DPO White Paper. We urge the WP29 to consider issuing guidance consistent with our recommendations on some of these issues as well, particularly the issues relating to the DPO's role as a strategic advisor and enabler of effective use of personal data; the related issue of the DPO's seniority and how this interacts with reporting to the "highest management level"; and the issue of cooperation and consultation with the DPAs. Thus, we suggest addressing the following items in the Guidelines:

- That the DPO may, in addition to performing his or her compliance function, also have the role of strategic advisor on the responsible, effective and innovative use of personal

[1] Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf.

data. This role can be effectively combined with the DPO's compliance role and reflects an existing trend borne out of practical experience in the industry. See CIPL DPO White Paper at Recommendation 10, p. 9 and Section 6.3(b), p. 34; see also discussion below at Section 2.c(i).

- That the DPO should, as a result of the wide range of expertise and skills required in this role, including any data strategy roles and ability to access the highest level of management, occupy a senior position within an organisation. See CIPL DPO White Paper at Recommendation 10, p. 9 and Section 6.3(b), p. 34.

- That the requirement of reporting to the "highest management level" should be interpreted pragmatically and flexibly to refer to "true" reporting lines to those within management that have authority to make relevant decisions and that organisations should be given appropriate leeway to operationalise this requirement within their own corporate structures. See CIPL DPO White Paper at Recommendation 11, pp. 11-12 and Section 5.1.2, pp. 27-28.

- That the issues of cooperation and consultation between the DPAs and DPOs are, in addition to being subject to the GDPR, also impacted by a number of competing considerations relating, for example, to legal privilege, duty of loyalty and other factors relating to the DPO's ability to be viewed as a trusted member of an organisation's team. Further elaboration on the WP29's understanding of these issues would be helpful. See CIPL DPO White Paper at Recommendation 16, p. 11 and Section 7(d) and (e), pp. 34-35. See also discussion below at Section 1.d(i).

Finally, we do suggest a few clarifications or modifications regarding the present DPO Guidelines at this stage, as indicated below.

CIPL's comments are organised under the headings used in the Guidelines document.

Comments

1. Designation of a DPO

   a. "Core Activities" (Section 2.1.2, p. 6)

The Guidelines list a number of examples of "core activities" that may require appointment of a DPO and "ancillary activities" that do not. CIPL agrees with the WP29's characterisation that while "ancillary activities" are "necessary support functions for the organisation's core activity or main business", they are still "usually considered ancillary functions" and, thus, do not trigger the designation of a mandatory DPO.

In addition to the examples of ancillary activities cited by the WP29—paying the organisation's employees and standard IT activities—there are other examples of typical ancillary activities,

which would be helpful to indicate in the Guidelines, as many controllers and processors have raised these examples in the past. They include (a) location data concerning delivery drivers in a B2B or B2C context or concerning maintenance service vehicles; (b) business and marketing communications; or (c) "monitoring of behaviour" in the IT and IS contexts, such as monitoring for cybersecurity purposes to protect the organisation's systems and assets (including IP, confidential information and personal data stored or processed by the organisation), and to comply with applicable laws and regulations (e.g. those relating to data protection, anti-fraud and anti-money laundering).

Recommendation: Add the above additional examples of "ancillary activities" to the DPO Guidelines—driver location data; business and marketing communications; and IT-related monitoring to further cybersecurity, protect systems and assets and comply with laws and regulations.

b. "Regular and Systematic Monitoring" (Section 2.1.4, p. 8)

With respect to the notion of "regular and systematic monitoring" of data subjects, the examples paragraph is overly broad, thereby risking to capture activities that may be "regular" and "systematic" but do not amount to "monitoring". It is important to clarify that some routine, systematic processing activities do not involve the monitoring of behaviour of individual data subjects and thus should not be considered as such. For example, operating a telecommunications network that involves routing individuals' communications in a regular and systematic manner does not constitute "monitoring of data subjects".

Another example may be loyalty programmes that do not involve monitoring behaviour (e.g. who eats what) but may simply provide bonus points based on the total value of purchased goods.

Similarly, IT tools designed to detect security and privacy breaches (such as DLP, SOC, SIEM) that are used to supervise network and server activity on an ongoing basis (i.e. "systematically"), (with potential monitoring occurring only in case of suspicious activity or incident), do not constitute regular and systematic monitoring of behaviour of data subjects. (And they also do not constitute "core" activities.)

The current examples in the Guidelines are too unspecific and could involve scenarios that should not be covered. Also, it is important to stress that these activities must be not only "regular and systematic" but also "core".

Recommendation: We recommend refining the examples, narrowing their scope to activities that actually involve monitoring of behaviour and that are "core" rather than "ancillary" activities. Alternatively, or in addition, the Guidelines might specify criteria for whether an activity is monitoring of data subjects.

c. DPO of the Processor (Section 2.2, p. 9)

Firstly, immediately above the examples, the WP29 states that "[i]t is important to highlight that even if the controller fulfils the criteria for mandatory designation, its processor is not necessarily required to appoint a DPO. This may, however, be good practice". While we agree with this statement, it would be good to provide some examples. The examples immediately below this paragraph do not cover this particular scenario. One possible example might be a controller in the health sector that processes health records and an IT service company that provides limited processing services regarding only pharmacovigilance data and events on a one-off basis. In that case, the controller's activity would be "core," but the processor's activity would not be "core" or "large scale".

Other possible examples may include:

- Generally, where a controller fully outsources its IT systems to an IT service provider with full access to the controller's personal data and databases, the IT service provider likely will need a DPO. However, in a situation in which the IT service provider provides only maintenance services on the systems/servers without having access to the personal data, or situations in which the processor does not even know if it is entrusted with personal data of the controller (cloud providers, for instance, in particular for infrastructure as a service [IaaS] offerings), a DPO appointment may not be required.

- In the case of an EU insurance company contracting with an email marketing campaign company to send marketing emails to prospective and current customers: The EU insurance company would require a DPO because it processes special categories of data on a large scale. The email marketing company would not be required to have a DPO because it is neither monitoring nor processing special categories of data.

Recommendation: Provide examples of the scenario where the controller must designate a DPO but the processor is not required to designate one.

Second, the WP29 recommends "as a matter of good practice, … that the DPO designated by a processor should also oversee activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics)". CIPL agrees that for the sake of avoiding confusion, both controllers and processors may want to have their DPOs (voluntary or mandatory) cover all data processing activities within the organisation, including, for processors, those with respect to which the processor is a controller in its own right. However, where certain processing activities not requiring a DPO can be treated separately without the risk of confusion, such as in the case of HR processing, organisations should be able to exclude such processing from the remit of the DPO and limit his or her scope to activities that triggered the DPO's mandatory appointment.

Recommendation: Clarify that where processing activities that do not require a DPO can be treated separately without the risk of confusion, organisations should be able to exclude such processing from the remit of the DPO.

d. Easily accessible from each establishment (Section 2.3, p. 10)

The WP29 states that the DPO "must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned".

The WP further states that "given that the DPO [referring to a single DPO designated for several public bodies] is responsible for a variety of tasks, the controller must ensure that a single DPO can perform these efficiently despite being responsible for several public authorities or bodies". (Emphasis added) The Guidelines then also refer to "[t]he personal availability of a DPO" (emphasis added) in connection with data subjects' ability to contact the DPO.

It would be welcome if the WP29 could clarify in this section that the DPO does not him- or herself have to have all necessary language skills. The current wording seems to assume that the DPO is one person and self-sufficient in the discharge of the relevant DPO tasks. The WP29 Guidelines recognize elsewhere that the DPO can rely on his or her internal or external support staff or team for performing the full range of the GDPR DPO tasks. Specifically, under "Necessary Resources" (Section 3.2, p. 13), the Guidelines provide that "[g]iven the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of the DPO as a team, under the responsibility of a designated lead contact for the client".

The fact that the DPO functions can be performed by a team is also recognized in the discussion of "DPO on the basis of a service contract" (Section 2.4, p. 12), noting that "individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients".

Clearly, without the ability to rely on an internal or external team, most DPOs will not be able to perform the full range of DPO tasks in multiple jurisdictions required by the GDPR, nor would they be able to satisfy easily all the qualifications and expertise requirements. For example, a DPO who resides outside the EU and speaks only English will have to rely on his EU-based team members to meet the language requirements addressed above. Similarly, a DPO will have to rely on the legal expertise distributed across his or her team in the various countries and jurisdictions in which the organisation operates. We believe that this is also the intent of the WP29 Guidelines, read as a whole.

Recommendation: Clarify that the role of DPO may be performed by an entire DPO team or the DP Office with respect to all GDPR DPO requirements, and qualifications, including with respect to knowledge of data protection laws and communication with data subjects and supervisory authorities in different languages. Of course, the formal "head" DPO would remain ultimately responsible for the tasks performed by his/her team members.

i. Secrecy or confidentiality (Section 2.3, p. 10)

In its discussion of easy accessibility of the DPO in Section 2.3, the WP29 also notes that "[t]he DPO is bound by secrecy and confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5))". It then notes that "[h]owever, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority." CIPL believes that this broad statement leaves many questions unanswered relating to the DPO's confidentiality duties vis-à-vis his or her organisation.

Recommendation: Clarify how the obligation of secrecy and confidentiality should be interpreted and applied in a way that ensures that (i) the DPO's loyalty to the organisation that appointed him or her is not compromised; (ii) the DPO's appropriate integration within the organisation as a "trusted counsellor" is preserved; and (iii) if the DPO is an outside lawyer to the organisation and the organisation's communications with him or her are protected by legal privilege, the DPO's legal duty of secrecy is protected.

e. Expertise and skills of the DPO – level of expertise (Section 2.4, p. 11)

i. Level of Expertise (p. 11)

The WP29 notes that the level of expertise of the DPO "must be commensurate with the sensitivity, complexity and amount of data an organisation processes". The WP then only cites to one concrete example of where a heightened level of expertise (or support) may be required: situations where organisations systematically transfer personal data outside the European Union. It is not clear why and how transfers outside the EU imply greater need for expertise than any other given data processing activity an organisation may perform that may require a certain expertise. Moreover, most organisations will, in one way or another, be involved in such data transfers, either within their own organisations or with third-party vendors or other business partners. Thus, an understanding of data transfers is becoming a basic necessity for all DPOs and privacy practitioners. Therefore, we don't believe such transfers merit being singled out.

Recommendation: Clarify that any processing activities, including cross-border transfers, may require heightened or specialised expertise, depending on context and make clear that cross-border transfers have no special status over other activities when it comes to assessing the required level of expertise of the DPO.

ii. Professional Qualities (p. 11)

The second paragraph in the Guidelines states that "[k]nowledge of the business sector and of the organisation of the controller is useful". This statement does not take into account that it is both common practice and essential for DPOs to be able to transition from one industry to the next. DPO mobility across sectors is both necessary in an environment where there is a shortage of experienced DPOs and actually useful in terms of increasing a DPO's general expertise and skill set. Thus knowledge of the business sector should not necessarily be viewed as one of the core professional qualities to look for in a DPO.

Recommendation: We suggest rephrasing or removing this item.

f. Publication and communication of the DPO's contact details (Section 2.5, p. 12)

The last sentence in paragraph 2 states that "the supervisory authorities can easily, directly and confidentially contact the DPO without having to contact another part of the organisation". It is hard to see how a DPA can contact the DPO confidentially without the DPO's subsequently having to discuss this with the organisation. This suggests some special relationship between the DPO and DPA that is not required by the GDPR, as well as being impracticable. Assuming the confidentiality of such communications would risk turning the DPO into a satellite regulator within the organisation. We don't believe this is the intent of the GDPR or the WP29 Guidelines.

Recommendation: We suggest deleting the phrase "and confidentially".

2. Position of the DPO (Section 3, p. 13)

a. Involvement of the DPO in all issues relating to data protection (Section 3.1, p. 13)

The Guidelines state that "[i]t is crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection". (Emphasis added). However, there are occasions related to data processing, such as minor privacy incidents, that do not rise to the level of requiring DPO involvement. Involving the DPO nevertheless would undermine the DPO's ability to prioritize and work on more important and material privacy and data processing issues. As recognized by the WP's Guidelines, the GDPR also provides that the DPO's involvement must be "proper and timely". This allows for an interpretation that minor data processing issues may not require immediate DPO involvement so long as he or she is ready to be involved and is involved at a proper time when and if an issue reaches an appropriate degree of importance. The criteria of when DPO involvement is needed could be set forth in the organisation's internal "data protection guidelines" recommended by the WP29 "that set out when the DPO must be consulted". Indeed, the WP's current phrasing implies that sometimes the DPO does not have to be consulted, but we suggest making it clear that organisations can establish their own escalation frameworks that define when a DPO will be actively involved. (It should also be clear

that "involvement of the DPO" can mean involvement by any of the DPO team members, as appropriate, rather than the formal "head" DPO him- or herself.)

Finally and importantly, the success of a data protection programme depends on data protection being embedded in the culture and practices of an organisation and on accountability and responsibility for data protection compliance vesting in all employees and functions of the organisation. It is the DPO's responsibility to educate other employees, raise awareness and provide self-help or self-service tools for use by employees and different functions in the organisation. Therefore, it is quite likely and should be encouraged that some non-material, non-high-risk data protection issues are dealt by other employees in the organisation.

Recommendation: Clarify that an organisation may establish criteria for exactly how and when a DPO (and DPO staff) must be involved in a data processing issue and that the DPO may not have to be involved in immaterial and minor data processing issues where the issues can be appropriately addressed by non-DPO staff.

The Guidelines also note that in cases of disagreement on data protection issues between the organisation and the DPO, it would be "good practice [] to document the reasons for not following the DPO's advice". Implementing this particular recommendation may have unintended negative consequences. For example, it may create (a) indirect pressures on DPOs to temper their advice or refrain from providing advice if they sense internal disagreement, lest they put the organisation in the difficult spot of having to create a problematic or negative record that could be used against the organisation in enforcement or litigation; (b) adversarial and uncooperative relationships between the DPOs and their organisations; and (c) lack of trust and openness between organisations and DPAs. While the GDPR generally requires that risk assessments, DPIAs, other accountability measures and other key processing decisions be documented and verifiable, it does not require the creation of a specific record of internal disagreements over the interpretation, for example, of a risk assessment prior to an organisational decision to proceed with the processing. What is required is that the organisation can show that the risk assessment supported its decision to engage in the processing and, where it fails to do so, to accept responsibility for a potential non-compliance. Moreover, where a risk assessment or a DPIA provides a suggested course of action based on the assessment and the organisation chose another course based on that same assessment, it is likely that there will be some existing documentation of where an organisation chose to diverge from a DPO's conclusions.

Recommendation: Further clarification of the scope and intent of this recommendation or removing it from the Guidelines.

b. Instructions and "acting in an independent manner" (Section 3.3, p. 14)

The second paragraph of the Guidelines states that "DPOs must not be instructed how to deal with the matter, for example, what result should be achieved, how to investigate a complaint or

whether to consult the supervisory authority" and "must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law". We understand and support what both the GDPR and the WP29 seek to guard against: that DPOs be told how to interpret the law or what the outcome of a risk assessment should be, or that they be encouraged to turn a blind eye to some data protection requirements. However, we believe that the Guidelines, as currently stated, may overstate what the GDPR requires in this regard and may be misunderstood. Certainly, the DPO has the authority and obligation under the GDPR to advise the organisation on data protection matters, which may include legal advice regarding such matters, free from the influence of the organisation. However, an organisation may decide, for example, that using legitimate interest as a ground for processing should be part of its general position and strategy where possible. It is hard to see how, in such a case, the DPO could not be instructed to consider and apply a legitimate interest ground for processing where possible. Of course, he or she could not be instructed on how to perform an analysis and what should be the outcome of a given legitimate interest analysis. Or, if, for example, legal advisors of the organisation suggest a certain line of action, it is hard to see how a DPO could not be instructed in that regard.

Recommendation: We recommend that the Guidance be refined to reflect the fact that, as part of a broader company ecosystem and as one of multiple organisational functions, all of which are subject to a management decision-making, the DPO can be instructed as to legal advice the company may receive or as to a company's general data protection strategy, including issues relating to the organisation's risk-posture, within which the DPO performs his or her compliance functions.

c. Conflicts of interest (Section 3.5, p. 15, n. 34)

i. The DPO as data strategist

CIPL welcomes the acknowledgement by the WP29 that determinations of conflict must be considered case-by-case, based on the specific organisational structure at hand. Such flexibility is key to the implementation of the GDPR's prohibition against conflicts of interest in a way that does not unnecessarily undermine the effectiveness and full potential of the DPO. However, the WP provides examples of potentially conflicting positions, including "roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing".

While this description is somewhat confusing and unclear, to the extent that it disapproves of a "data strategist" function of the DPO, we strongly suggest reconsideration. Effective DPOs frequently perform the role of chief data strategist and enabler of effective data use and innovation, a function that is naturally interknit with and dependent upon applicable data protection requirements. The DPO is often in the best position to balance and integrate privacy compliance functions with the effective and strategic use of personal data and DPOs can perform these two interdependent functions without experiencing conflicts of interest.

Additionally, the phrase "lead to the determination of purposes"(emphasis added) is somewhat unclear because it leaves unanswered whether the objection is to a DPO's making purpose decisions him- or herself or merely advising others on what decisions to make. Most likely, a DPO who also performs data strategy functions would merely advise organisational leadership on such issues. Thus, while it may be difficult to reconcile the task of making purpose decisions with the DPO role because that role includes assessing such decisions, this is not the case when a DPO merely advises on these issues.

Recommendation: Remove the objection (if any) to the DPO's also performing data strategy functions within an organisation and/or clarify the intent of this particular item in footnote 34 if an objection to a DPO's data strategist role was not intended. Also, it would be appropriate to state affirmatively that a data strategy function is not inherently in conflict with the compliance functions of a DPO. In addition, it may make sense to move the examples in footnote 34 into the main text.

ii. The DPO as ISO or CIO in the context of SMEs

The same discussion on conflicts of interest, particularly the statement concerning positions that "lead to the determination of purposes and means of processing" also casts doubt on whether a DPO could also serve as an information security officer or chief information officer. We note that this may pose significant challenges for SMEs that may have to rely on limited staff to perform multiple related roles.

Recommendation: Clarify that the role of the DPO may be combined with the role of an ISO or CIO, particularly in the context of SMEs and if conflicts of interest concerns are properly addressed.

3. Tasks of the DPO (p. 16)

a. The DPO's role in record-keeping (Section 4.4, p. 16)

The Guidelines correctly point out that under the GDPR it is the controller's or processor's obligation to maintain processing records. However, the Guidelines then state that "DPOs often … hold a register of processing operations based on information provided to them by the various departments in their organisation". We note that this is not correct in all member states. In fact, there is a tendency for a DPO not to perform such a task, but to rely on other functions in the organisation to hold such records, including IT and CIO functions.

Indeed, record-keeping usually is a cross-business effort and is necessarily so. It is not likely to be a Word document held by a DPO. Rather, it is likely to be a collection of records, documents and information from across the business that are kept in different formats, using different software, on different systems. It requires information from and records held by IT on what data is in what systems, who the information asset owners are, data flows, etc.; plus

information from and records held by business areas on uses made of data, disclosures of data, additional local storage of data, etc.; plus information provided by the legal department of the DPO on what condition for processing is being used, whether there is sensitive data, etc. It will also include corporate documents such as retention schedules, and many more types of documents and records. These documents and records just need to be accessible to the DPO via company systems.

Thus, we believe that the WP29 should not suggest that the DPO should keep the "register", as the register requirement may distract from other many more important duties of the DPO and would take up significant time and resources of the DPO that can be better deployed elsewhere.

Recommendation: We suggest deleting the reference to DPOs' performing this function, leaving it to the organisations to decide who holds such registers.

Conclusion

Thank you for the opportunity to provide further comments on key DPO implementation questions. To the extent the WP29 decides to accommodate all or some of our suggestions, we would assume you would also update the associated Frequently Asked Questions. We look forward to providing further input on the DPO Guidelines in the future as new issues arise, particularly in light of any practical experiences in applying the GDPR DPO requirements. In the meantime, please do not hesitate to contact us for further information or clarification at bbellamy@hunton.com; mheyder@hunton.com; and hhijmans@hunton.com.