Centre for Information Policy Leadership
Hunton & Williams LLP

30 ST MARY AXE
LONDON EC3A 8EP
TEL +44 (0)20 7220 5700
FAX +44 (0)20 7220 5772

2200 PENNSYLVANIA AVENUE
WASHINGTON, DC 20037
TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

CIPL and its GDPR Project Stakeholders Discuss DPOs and Risk under GDPR

In September, the Centre for Information Policy Leadership ("CIPL") held its second GDPR Workshop in Paris as part of its two-year GDPR Implementation Project. The purpose of the project is to provide a forum for stakeholders to promote EU-wide consistency in implementing the GDPR, encourage forward-thinking and future-proof interpretations of key GDPR provisions, develop and share relevant best practices, and foster a culture of trust and collaboration between regulators and industry.

Since the inaugural workshop in March 2016 in Amsterdam, participation in the project has grown significantly. The workshop was attended by almost 120 delegates from businesses, 12 data protection authorities ("DPAs"), four EU Member State governments, the EU Commission and the European Data Protection Supervisor, a non-DPA regulator, several academics and the IAPP. The fact that now over 70 companies are involved in this project speaks to the importance of the topic and the need to coordinate and benchmark among impacted stakeholders across the various sectors, in light of the tight deadline of May 25, 2018, when the GDPR becomes fully applicable.

The Paris workshop focused on two key areas under the GDPR: the role of the data protection officer ("DPO") and the risk-based approach in the application of the GDPR (i.e., in connection with data protection impact assessments ("DPIAs")). Both reflect key priorities of the Article 29 Working Party ("Working Party") for developing its own GDPR implementation guidance, as well as the high importance of these two areas for the industry. Additional topics will be covered in future phases of the CIPL project.

Overall, the discussions of the day were a productive mix of a reality check, a wake-up call and encouragement. Particularly promising were instances of emerging consensus around several key implementation questions. While the discussions illustrated how many provisions under the GDPR remain unclear and how much work is left to be done before the quickly approaching implementation deadline, it was reassuring that no one seemed to be slow-pedaling their respective implementation responsibilities. Instead, we saw concentrated energy and commitment from all sides. There was a sense of shared responsibility for the successful and timely implementation of the GDPR between industry, DPAs, national governments and the EU Commission. Finally, it was also recognized that the lines of communication between regulators, industry and other stakeholders should stay open to ensure the best outcome for everybody.

Forthcoming Working Party GDPR Guidance
We learned that the Working Party will be releasing its first round of GDPR guidance before the end of the year or, at the latest, beginning of 2017, on data portability and the role of the DPO. Subsequently, the Working Party plans to release guidance on risk,

DPIAs and certifications. Also, the Working Party is on the verge of publishing the report from its first GDPR "FabLab" meeting in July 2016.

The GDPR Represents a Revolution, Not an Evolution
A non-private sector participant also posited that the GDPR represents more of an "evolution" than a "revolution." The predominant view, however, expressed not only by industry, was that "revolution" was the more accurate term. The familiar concepts of the GDPR will have to be interpreted against a backdrop of a changing technological and digital environment. Also, many of the new obligations for industry and DPAs will require a comprehensive retooling of organizational privacy programs and regulatory enforcement structures, among other changes. Participants stressed the need for timely guidance, frequent updates and full transparency from both DPAs and EU Member States during the implementation process.

EU Member States and DPAs Are Pressing Forward on National Implementation
A *tour de table* by all present EU Member State representatives and DPAs to update on their progress on national implementation of the GDPR drove home the sheer magnitude and complexity of the involved tasks. They included (1) reviewing the existing data protection laws and updating them in light of the GDPR; (2) coordinating among relevant government bodies; (3) considering how to deal with the margin of maneuver for EU Member States under the GDPR in various clauses; (4) resourcing and restructuring the DPAs for their expanded responsibilities; (5) developing implementation guidance; and (6) coordinating across EU Member States, for example via the Working Party and the European Commission.

The public sector delegates, who are personally involved in the national implementation and transition work, are keenly aware of the challenges facing the industry as it tries to come into compliance by May 2018. Among other things, these representatives pointed to corporate budget cycles that define and circumscribe the resources that will be available for GDPR implementation over the next 20 months even though the necessary resources cannot properly be calculated given the uncertainties of what the GDPR requires.

The Role of the DPO
The first main discussion of the day concerned the practical implementation of the new DPO obligations. Some of the key takeaways on which there appeared to be general agreement amongst a plurality of the present stakeholders included the following:

- The GDPR **expands the traditional compliance function** of a data protection officer to a **broader, more strategic role**, including that of business advisor on the responsible and innovative use of personal data. Given the various functions and skill-sets that must be combined in the DPO, they can be described as a *chef d'orchestre* with respect to an organization's strategic use, management and protection of personal data. Certainly, the DPO should not be viewed as an internal "police officer"; a "privacy champion" might be a more fitting description.

- The DPO **must be one person** who is responsible for data protection within the organization, but the relevant DPO **skills and expertise** required by the GDPR can be drawn from the **entire DPO team** across multiple jurisdictions. "Cloud expertise is good, cloud responsibility is not good," one of the DPAs noted.

- A **non-mandatory (or voluntary) DPO** appointed under Article 37(4) must meet all of the DPO requirements of the GDPR.

- Some organizations may not wish to appoint a **DPO if they are not legally required** to do so under the GDPR. If an organization that is not legally required to appoint a mandatory DPO under the GDPR nevertheless wishes to create a data protection role or function within the organization outside of the GDPR requirements, it must give that role or function a different name, such as "Chief Privacy Officer," or "Data Protection Director or Lead." (The title of "Data Protection Officer" has now been claimed by the GDPR).

- Generally, DPAs should find ways to **incentivize the appointment** of a DPO or a person with equivalent responsibilities for all organizations, including SMEs and start-ups.

- The criteria of "**core activities**," "**regular and systematic monitoring**" and "**large scale**" as triggers for mandatory DPO appointment under the GDPR cannot easily be further clarified and defined by additional objective, external criteria. For the most part, their application must be flexible and context-specific and left to the judgment of the organization deciding whether a DPO is required, keeping in mind that organizations must be able to demonstrate and justify their decisions.

- "**Core activities**" **does not include** monitoring of employees or other parties on the company's premises (IT monitoring and/or video surveillance), including monitoring of company emails, assets and systems for security purposes; the use of analytic tools for purposes, such as understanding customers' use of online products or to improve products or workforce allocation; and activities required by law.

- It does not matter **where the DPO is located geographically** as long as there is effective implementation of the GDPR requirements, including those relating to the organizational reporting lines pertaining to the DPO and the requirements relating to DPO accessibility to individuals and DPOs.

- A DPO does not need to be in the location of the organization's main establishment and lead supervisory authority.
- **Accessibility of the DPO** to individuals can be provided via local DPO staff or technology.

- The GDPR does not provide for **personal liability** of the DPO. This makes sense in light of the fact that, under the GDPR, the DPO is, in essence, an internal advisor and the controller is responsible for data protection decisions. Most participants agreed that imposing personal liability on DPOs would not be helpful. However, EU

Member States' law (such as criminal or corporate law) could impose additional liability or penalties.

- It is not the DPAs' responsibility to create or impose further DPO qualification standards or certifications. To the extent **DPO certifications** are desired, they should be developed by the market. Universities could play a role. However, DPAs have a role in encouraging such certifications and helping to create networks of DPOs.

- **Formal certification** should not be required for DPOs; instead, hiring organizations should be able to use their judgement and consider the general experience and knowledge of a DPO candidate on a case-by-case basis.

- **An external DPO could be a legal person**; however, an individual has to be the main contact.

- External DPOs are a valid choice for **SMEs and start-ups**.

- The DPO's task of "**monitoring compliance**" within an organization is not a formal audit function that could potentially be at odds with the task of "advising" the organization, but refers to the DPO's obligation to oversee and ensure on an ongoing basis that the organization implements all applicable GDPR requirements.

- The DPO's "**consultation**" **role** with respect to the DPAs (including "prior consultation" regarding high-risk activities) is important, but there is an expectation on the part of DPAs that such consultations are the exception rather than the rule. DPAs are not resourced for frequent consultations. On the other hand, industry confirmed that there is a need for on-going informal consultation and constructive dialogue between the DPO and the DPA. This should be encouraged by both sides.

Risk, High-Risk and DPIAs

The second major issue of the day was the role of risk under the GDPR. Specifically, participants discussed possible interpretations and further guidance relating to the nature and methodology of risk assessments, including in connection with DPIAs. Key takeaway and messages included the following:

- There was consensus that considering the **benefits** of a data processing activity should be part of a GDPR risk assessment. Benefits are relevant both in the context of devising appropriate mitigations (so as to avoid mitigating the benefits away) and when deciding whether to proceed with processing, given the residual risk.

- Article 35(1) provides that **DPIAs** are only required once with respect to "**similar processing operations that present similar risks**." This is designed to prevent unnecessary and duplicative DPIAs. Any further guidance on DPIAs should highlight this important feature and clarify its meaning and application.

- Article 35(3) sets forth three apparent "**default**" **high-risk categories** that automatically require a DPIA. A question was raised as to whether this "high-risk" classification can be rebutted based on the "nature, scope, context and purposes" (Article 35(1)) of the proposed processing at issue before reaching the DPIA stage. Future guidance might address this question.

- "**Using new technology**" cannot be the sole trigger for "high-risk" status or a DPIA. This criterion must be coupled with additional "high-risk" triggers that depend on nature, purpose, context and scope of processing. Any future guidance should narrow the scope of what is meant by "new technology." Otherwise, almost every new data processing activity is captured by it.

- **Further guidance on** "**high risk**" from the DPA should not be too "bureaucratic." It should feature characteristics and criteria of "high risk" rather than a list that specifies *per se* "high-risk" activities. Prior consultation with stakeholders before releasing final guidance on the meaning of "high risk" would be helpful.

- Flexibility in determining how to score, measure and weigh the risks and benefits in a specific processing context is key and should be left to individual organizations. Also, no specific **risk assessment process or methodology**should be mandated. However, high-level guidance on the general contours of a risk assessment methodology or process might be helpful.

- The Working Party may base its further guidance on **existing DPIA guidance** by national DPAs.

- Considering **appropriate mitigations** requires taking into account the reasonable expectations of individuals, transparency and the elements of fair processing.

- "**Prior consultations**" with DPAs regarding DPIAs that demonstrate "high risk" despite mitigations should be the exception rather than the rule.

- There may be future DPA guidance on mitigation measures by way of "**mitigation scenarios**."

- Many organizations roll out new products globally without variation between countries. Thus, risk assessments must comprehensively **assess the global impact** of a product. Any further DPA guidance on the elements and methodology of risk assessment must be workable in that context.

- The GDPR provides for "seeking the views" of individuals or their representatives in the context of a DPIA "where appropriate." This obligation must be limited by the organizations' commercial interests, IP rights and security considerations. Future DPIA guidance should acknowledge that under common product roll-out practices, for example, there may not be an opportunity for prior consultation with individuals

before such roll-out. However, in some circumstances feedback from individuals, including on user experience, may be obtained during pre-roll-out limited testing phases.

- The **original intent behind the risk-based approach** was to enable broader, but more accountable, use of personal data. If the GDPR's risk-based approach is implemented in an overly bureaucratic fashion, it runs the risk of merely adding compliance obligations without any corresponding benefits in terms of effective, innovative and accountable data use.

Risk-based Enforcement and Oversight by the DPAs
Workshop participants also considered how the risk-based approach might enable more effective data protection oversight and enforcement by the DPAs. This discussion was designed to kick off a new work stream within CIPL's GDPR Implementation Project that will specifically explore the issue of "smart regulation."

In a nutshell, this discussion was premised on the idea that DPAs will not be able to fulfill all the new tasks, powers and functions assigned to them by the GDPR, unless they make choices and set priorities. It was pointed out that while the GDPR does not explicitly ask for prioritization based on strategic importance or impact, DPAs must, nevertheless, make realistic and prudent choices. One mechanism to facilitate such choices would be to apply the risk-based approach to the DPAs' various tasks and responsibilities, enabling them to prioritize actions according to risk, importance and impact.

By way of an example, the participants considered the DPA's role as an ombudsman for complaints. This role, arguably, is the least important among the other roles of the DPA, such as "leader," "authorizer" and "enforcer." Yet, depending on the volume of complaints (many of which could be of limited importance or merit), the ombudsman role has the potential for monopolizing the time and resources of the DPAs, thereby limiting their ability to perform their other functions effectively.

As mentioned, solutions to this and other problems relating to DPA effectiveness will be the subject of the "smart regulations" works stream. By incorporating the concepts of organizational accountability, the risk-based approach and certifications and codes of conduct, the GDPR's ambition was to enable organizations to do better in the future, to share the regulatory burden with DPAs and, ultimately, to better protect individuals. Whether all this will be sufficient to obviate the DPAs' need to prioritize remains to be seen. Better to cover all bases and plan for responsible risk-based prioritization amongst all stakeholders.

Next Steps
To do our part in enabling timely GDPR compliance, CIPL will finalize two white papers and formal recommendations concerning the DPO and risk in the coming weeks and then turn to our next set of priority issues under the regulation, including certifications and codes of conduct, innovation drivers, consent/legitimate interest, transparency and smart regulation.

The next, smaller multistakeholder workshop will be in Brussels on November 8, 2016, on the issue of certifications and codes. Afterwards, the next major GDPR Project workshop will be in February or early March in a European location to be determined.