The following comments are pursuant to the Article 29 Working Party’s request for comment on the proposed “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679” (“Guidelines”).

The Information Accountability Foundation (“IAF”) welcomes the draft Guidelines from the Article 29 Working Party and commends the Article 29 Working Party for the Guidelines’ completeness. The IAF offers suggestions based on the research it has conducted on comprehensive data impact assessments and their use to isolate risk and balance the interests of the various stakeholders impacted by the processing of data. The IAF makes its recommendation not to add any additional controller requirements but rather to place DPIAs in the context of a comprehensive, accountable data protection program.

IAF Background

The IAF is a non-profit organisation whose charitable purpose is research and education. It was founded in 2013 to further the work of the Global Accountability Dialogue that formulated the Essential Elements of Accountability. The IAF has a global mission and has been active in Europe since its founding.

The IAF recently completed a project, partially funded by the Office of the Privacy Commissioner of Canada, on a framework to assess big data analytics to determine whether they are legal, fair and just (the “IAF Canadian Research”). Canadian private sector privacy law, The Personal Information Protection and Electronic Documents Act (“PIPEDA”), requires there to be permission to process data, most often through consent, as well as an organisation to be accountable. The IAF Canadian Research was responsive to the accountability provisions of PIPEDA when conducting complex data processing. In this way, the IAF Canadian Research is applicable to the implementation of the General Data Protection Regulation (“GDPR”).¹ These comments will reference the IAF Canadian Research.

The IAF is currently developing a comprehensive assessment process to meet the balancing test required by the legitimate interest legal basis to process as part of the GDPR, and the IAF sees significant alignment between that assessment process and DPIAs. The IAF will share that assessment framework with the Article 29 Working Party when it is completed later this year.

IAF’s comments are also based on research dating back to 2012 and accountability concepts dating back to 2009.

Generally, the IAF finds the Guidelines helpful and mostly complete. The IAF’s comments are mostly additive.

Nature, Scope, Context and Purposes are Significant to Understanding Risk

All processing of personal data creates risks. All risks must be assessed with an eye to the overarching objectives of the European Union to bring about “constant improvements of the living conditions of their peoples.”2 Society tolerates some level of risks when processing creates outcomes that contribute benefits to individuals, groups of individuals, society, and the controllers that process the data. That is why GDPR Article 35(6)(a) requires a systematic description of the processing. Such a systematic description not only describes the mechanics of how processing might take place but also the value that will be created by the processing and which stakeholders benefit from that value.

The IAF Canadian big data assessment process asks controllers to identify the stakeholders impacted by a complex processing, the benefits created by the processing, the risks associated with a processing, and whether the benefits are going to the stakeholders that bear the risk. It is through this process that one begins to see what is necessary and proportional consistent with GDPR Article 5(1)(c). The Canadian guidance rank orders the stakeholders’ interests, placing the individual first, followed by groups of individuals and society, with the controller last. Whether the processing is necessary or proportional, risks to individuals still need to be mitigated when possible, and where risks are still significant, a consultation with the appropriate authority is required. However, it is this assessment process that assists the authority in determining that the value created by the processing makes the risk tolerable.

The GDPR was legislated to protect the fundamental right to data protection. The GDPR looks to the full range of fundamental rights and freedoms and is designed to meet the objectives set by EU treaties. IAF works leads it to believe that the concept of context requires that risks and benefits be assessed concurrently.

Data Impact Assessments Are Part of the Controller being Responsible and Answerable

There is no question that the GDPR requires controllers to know both when a DPIA is necessary and when it is necessary to conduct one, as required by Article 35. The requirement for a controller to be responsible is set forth in Article 24. Responsible is half of the definition for accountability; the other half is being answerable, which is required by Article 5(2). The concept of assessments as an accountability process was established by the “Essential Elements of Accountability,” 3 published by the Global Accountability Dialogue in 2009, and is the basis for the Article 29 Working Party accountability opinion published in 2010. Essential element 2, that covers mechanisms to put policies in place, says such mechanisms should include assessments to identify the risks associated with processing. Since 2009 the Global Accountability Dialogue, the Centre for Information Policy Leadership (that formerly housed the Global Accountability Dialogue), and the IAF have been exploring assessments. We have found that assessments meet a governance need that supports compliance. This governance need is

---

2 Treaty on the Functioning of the European Union.
directly responsive to Article 24 which states “taking into account the nature, scope, context and purposes” of a processing. It helps controllers not only understand the risk that they create for others, with an emphasis on data subjects, but also understand whether a processing meets real needs for the organisation and other stakeholders. By conducting such an assessment, the controller establishes that the processing is legitimate and responsible, especially when the legal basis for the processing is something other than consent.

From a data governance perspective, the IAF sees a data protection office review as a means of allocating resources to manage and mitigate risks thoughtfully. This review means assessments should be scalable to risks and complexity. At the first level, this review means a simple inquiry to determine whether the processing is a continuation of a process that has already been assessed, is straightforward or does not involve any inherently high risks to individuals. In that case, no additional assessment might be necessary. Where there are issues that are fairly simple, an assessment that looks mostly at data security, retention, cross-border data transfer, individual rights management and other technical privacy requirements, might be all that is necessary. Where the processing is complex, uses data from numerous sources, or raise the issues covered in the Guidance, then a full comprehensive data impact assessment would be necessary, including an assessment of benefits and impacts, risks and mitigation.

The IAF Canadian Research made use of this triage process. Privacy Impact Assessments ("PIAs") are well established as part of the accountability guidance published by the Federal Office of the Privacy Commissioner and the Information Commissioners in British Columbia and Alberta. However, PIAs are based on fair information practice principles. The Canadian assessment process added complex processing questions to the basic PIA for when organisations are conducting complex processing such as big data.

The concept of tiered assessments is also responsive to ongoing European discussions on ethical processing being led by the European Data Protection Supervisor and others. The IAF research shows that a family of assessments is the lynchpin of a comprehensive accountability based data protection program.

The Role of the DPO in DPIAs

The IAF, as part of its research, has looked at how many controllers conduct assessments of various levels of complexity. At some organisations the assessments are conducted by business units based on instructions from privacy offices, while at other organisations the assessments are actually conducted by the privacy office with the participation of the business units. The mechanics of the assessments are based on the business processes of the respective businesses. Organisations with both models participated in the IAF Canadian Research. The IAF has seen both models be effective.

The GDPR requires some organisations to have a Data Protection Officer ("DPO"). The GDPR also allows this function to be structured as the Office of the DPO with functionality distributed in a team. The Guidelines require the DPO be consulted by the controller as it conducts the assessment. Implicit in this requirement is the role of the DPO, or office of the DPO, to be both a participant and judge of whether the assessment was conducted in an honest and skilled fashion. As the office of the DPO matures under
the GDPR, numerous offices of the DPO will be the actual conductors of the DPIA for the organisation. The IAF does not believe that the Guidelines preclude this type of structure.

Again, the IAF thanks the Article 29 Working Party for the opportunity to submit these comments. Any questions related to these comments should be sent to Martin Abrams at mabrams@informationaccountability.org.

Martin Abrams
Executive Director