19 January 2018

The following comments are pursuant to the Article 29 Data Protection Working Party ("WP29") draft guidance entitled "Guidelines on Transparency under Regulation 2016/679" ("Draft Guidance"). The Information Accountability Foundation ("IAF") welcomes the opportunity to file comments on this important regulatory process.

Transparency is essential to the effective operation of the General Data Protection Regulation ("GDPR"). It informs the ability of people to exercise their rights, facilitating oversight and giving the public a sense of whether information is managed in a manner that assures the full range of fundamental rights and freedoms articulated by the various EU treaties. Transparency is a challenge that grows more difficult as communication and computing technologies become more complex. Useful guidance should provide a sense of expectations or objectives, without limiting the means for reaching those expectations. Final guidance will be judged based on how well this balance is achieved.

IAF Background

The Information Accountability Foundation ("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. These comments have been developed by staff strategists and do not necessarily reflect the views of the IAF board of trustees or funders.

As the Draft Guidance mentioned, transparency is not a new requirement, and it is not one that is new to the IAF staff. Chief strategist Martin Abrams has been involved in research on effective transparency since 2001 when he led the "Simplified Notices" project at the Centre for Information Policy Leadership. As part of leading that project, Mr. Abrams led a session at the International Conference of Data Protection and Privacy Commissioners in Sidney in 2003 that resulted in a conference resolution on the adoption of simplified notices. He co-chaired a working meeting on simplified notices in Berlin in 2004, co-chaired by the then current commissioners for Australia, Malcolm Crompton, and for the United Kingdom, Richard Thomas. Lastly, Mr. Abrams was a lead author on guidance on multi-layered notices published by the OECD in 2008.

The entire IAF team has worked on industry or corporate transparency challenges that have ranged from privacy notices for financial instruments to the cultural differences between communicating privacy in different global communities.

Important Endeavor

The IAF notes that the Draft Guidance is not secondary regulation but rather a commentary on legal requirements mandated by the GDPR that go into effect in May. WP29 draft guidance, and IAF comments on that guidance, are interpretive on how best to meet both the letter and spirit of the GDPR.

The IAF team appreciates that the Draft Guidance is one of numerous guidance documents being developed by the WP29. The challenge of translating the 173 recitals and 99 articles of the GDPR into practical guidance that might advise businesses of all sizes and types in a community with many language, cultural and contextual differences is daunting. While all of the guidance documents are complex, maybe none is as complex as the challenges associated with educating people about the data and data uses associated with ever evolving communication and computing technologies. The team that developed the Draft Guidance is to be congratulated for its completeness. These comments are respectful of the great efforts and skills put forth by that team.

Expectations versus the Cost of Meeting Those Expectations

Knowledge about what organisations are doing with the data that pertains to individuals, and how those individuals may exercise their rights, is very important to the overall GDPR compliance approach. The Draft Guidance creates expectations that organisations will expend the resources necessary to have the best possible chance of connecting with individuals. To meet those expectations, organisations of all sizes and complexity will need skills, resourcing and differing capabilities and capacity to achieve the preferred transparency. For example:

- Communications specialists with expertise in data protection to describe (in partnership with the data protection leader) data processing activities and user rights, in simple age- and consumer-appropriate language, and to accurately describe data breaches (in partnership with data protection and security leaders) to impacted data subjects and enforcement agencies;
- Consumer research staff to test timing and efficacy of language and transparency delivery including multi-language translations;
- Experienced designers and programmers to create the needed online and in-product experiences, product flow and visual design that are 'just-in-time' or to describe further data processing activities when they arise.

It will be equally critical for organisations to put into place new business processes to ensure consistency across the recommended communications channels recommended by the Draft Guidance. A limited number of organisations have these skills in place, but most do not. Putting such resources in place will require a substantial investment that needs to be balanced against other expectations, with the knowledge that only the most motivated individuals will have the time to absorb the communications. It may be useful for the WP29 to place transparency expectations in the context of the other requirements of the GDPR.

Basic Conundrum

Moreover, there is a basic conundrum associated with the challenge of making transparency simple and concise on the one hand and complete on the other hand.

As the Draft Guidance makes clear, transparency has many functions, but the two most important functions are: to facilitate trust by making it possible for people to understand the processing of data

that relates to them that will take place and why they may see it as fair, and to inform people so they may exercise their rights as they relate to processing of personal data. The Draft Guidance also makes it clear that transparency goes well beyond privacy notices that might inform consent.

The Draft Guidance is also crystal clear that transparency is not new to data protection. Originally, transparency was intended to inform the transfer of control from an individual to a controller. This simple mechanism for control was very reasonable when databases and data flows were few and far between. That, as the Draft Guidance makes so clear, is not the situation today. Data uses are complex, and there are multiple uses for the same sets of data. All processing must be legitimate, and none may be secretive.

Furthermore, data origination may be direct with the individual, off a device on or even in the individual, or may be the byproduct of an earlier processing. The uses for that data may be very complex, such as information related to the interaction between medical devices.

While nothing should be secret, not everything will be easily explainable. As the Draft Guidance says, it must be concise, transparent, intelligible and easily accessible. It must be conveyed in clear and plain language. The items that must be conveyed are numerous.

The conundrum lies not in the objectives for transparency but rather in the details deemed necessary to achieve those objectives. The Draft Guidance includes a table with 14 different factors necessary for compliant transparency. A table with 14 factors seems contradictory to concise and simple. While this conundrum partially comes from the GDPR itself, a useful question is whether the Draft Guidance has made the complexity less complicated or more complicated for organisations of all sizes that must comply with the GDPR?

The challenge lies not in communicating all the factors as required by the GDPR but rather in the implementation of these factors due to the prominence of some factors over others. Prioritising these factors requires judgement on the part of controllers, and then an editorial process that establishes prominence based on context, based on sound work by corporate data protection staff. Large, mature organisations probably have the resources to traverse this knotty minefield, but small and medium size organisations will be hard pressed to parse the Draft Guidance let alone implement it.

<u>Alternative Ways of Thinking of Transparency Strategy</u>

Alternatively, to make the approach toward transparency less complex, the WP 29 might view the management of transparency as part of the accountability requirement under the GDPR, something the Draft Guidance contemplates in Section 2. Accountability is related to the full range of activities with regards to a complete data protection management program. An accountability approach associates transparency to the context of the relationship of the individual to the organisation. So rather than just being a legal exercise, transparency would be a data protection management endeavor. One would fall back on the clear objectives for accountability, and by extension transparency, and let the organisation figure out the strategy for conveying these objectives most effectively consistent with the plain text in the GDPR. This approach goes to the Draft Guidance setting expectations rather than mandating means. This approach also goes to the Draft Guidance making clear that an organisation must think through the prominence dedicated to some requirements over others.

Accountability also requires an organisation to stand ready to demonstrate the management steps taken to comply with the requirements of the law. In this case, compliance with the legal requirements is the rank ordering of what is presented and the explanation by the accountable organisation. The regulator would then oversee whether the organisation's implementation of a transparency plan was done with integrity and competence.

Avoiding Reticence Risk[1]

The GDPR is part of the European Union strategy for one digital market that is an engine for employment and economic growth. The GDPR is intended to create both legal certainty and a platform for the free flow of data in a suitably protected manner. This strategy is responsive to all the stakeholder rights and interests articulated in the treaties that have established the European Union.

There are various provisions in the GDPR that are intended to create flexibility for discovering new knowledge, including new and better means for achieving stakeholder objectives. Article 5(1)(b) is one such provision. It states: "[personal data shall be] collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, . . ., not be considered to be incompatible with the initial purpose." The IAF team is concerned that the Draft Guidance focuses on the first part of that sub-article but not the second half of it.

The Draft Guidance focuses on the need for organisations to be very specific in stating all the purposes and the legal basis for all such purposes. New processing may develop over time that is not inconsistent with the original purposes. The GDPR was not intended to stifle innovation through work flow improvements that are not inconsistent. The IAF is concerned that the Draft Guidance may create reticence risk related to new processing that is not incompatible with the initial processing.

The concern rests in the example under Section 11 of the Draft Guidance. The example says, "the following phrases are not sufficiently clear as to the purposes of processing," and includes "we may use your personal data for research purposes" as one that is not sufficiently clear.

While IAF can see where greater clarity would be optimal, what would the more honest statement be if the research necessity evolves over time? Concern exists that beneficial processing that is not inconsistent will not be conducted because it was not communicated previously.

Closing

The IAF appreciates the opportunity to comment on the Draft Guidance. Questions may be directed to Martin Abrams, executive director, mabrams@informationaccountability.org.

[1] Reticence risk is the concern that processing that will result in beneficial activities will not be done because organisations are not clear whether they can resolve the regulatory and reputational risk associated with the processing.