Data Protection Privacy Impact Assessments

A Data Protection Impact Assessment (DPIA) is designed to assist BCO in assessing the risks associated with data processing activities that may pose a high risk to the rights and freedoms of individuals and is a requirement of Article 35 of the GDPR.

The Article 29 Working Party, consisting of the representatives from each data protection authority in the EU, has published guidelines on DPIAs and whether processing is likely to result in a high risk for the purposes of the GDPR. In assessing whether processing is likely to result in a high risk the Article 29 Working Party has set forth the following criteria to consider:

- Evaluation or scoring, including profiling and predicting, especially "from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (recitals 71 and 91). Examples of this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
- Automated decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35 (3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.
- Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area"(Article 35 (3)(c)). This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publically accessible) space(s).
- Sensitive data: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offenses. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the data has already been made publically available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email

services, diaries, e-readers equipped with note taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be considered as very intrusive.

- Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
    - The number of data subjects concerned, either as a specific number or as a proportion of the relevant population
    - The volume of data and/or the range of different data items being processed
    - The duration, or permanence, of the data processing activity
    - The geographical extent of the processing activity
- Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
- Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management. Similarly, children can't be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segments of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
- Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that use of a new technology can trigger the need to carry out a DPIA. This is because the use of a new technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.
- Data transfer across borders outside the European Union (recital 116), taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers, or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91). This includes processing's performed in a public area that people passing by cannot avoid, or processing's that aims at allowing, modifying or reusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.