João Alfredo Afonso Partner
joaoafonso@mlgts.pt

Pedro Verde Pinho Associate
pvpinho@mlgts.pt

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Data Protection Impact Assessments under the GDPR: questions unanswered?

25 May 2018 is just around the corner, and with it comes the application of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). The GDPR brings onto the scene a set of novelties, which leave a series of questions still unanswered. One of the novelties are Data Protection Impact Assessments ('DPIAs'), which have been made mandatory in some circumstances under the GDPR. Although many organisations have been performing these prior to the existence of the GDPR, its requirement will have a particularly large impact on data protection governance within companies and will raise a significant number of complex questions, as highlighted by the Article 29 Working Party's ('WP29') recent focus on the matter. João Alfredo Afonso and Pedro Verde Pinho, Partner and Associate at Morais Leitão, Galvão Teles, Soares da Silva & Associados, examine the issues raised.

Introduction

Also known as Privacy Impact Assessments, the WP29 defines the procedure as "a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data," that is to say, "a DPIA is a process for building and demonstrating compliance[1]."

The GDPR establishes the compulsory requirement of undertaking DPIAs when a type of processing using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, considering the nature, scope, context and purpose of the processing. Some of the questions raised by this provision on DPIAs have already been posed by the European Data Coalition in their 'Recommendations on the Implementation of the GDPR[2],' such as the lack of a clear definition of what constitutes 'risk' and 'high risk' and when a prior consultation must be made.

WP29 guidelines

The WP29 addressed these issues in their recent guidelines on this subject, which were published for public consultation with the purpose of determining, in particular, what should be understood as 'a processing that is likely to result in a high risk,' as it is unclear when this procedure is mandatory, except for the three specific cases set forth in Article 35(3) of the GDPR.

For this purpose, the WP29 laid out in the abovementioned guidelines the following ten criteria that organisations should consider when determining whether the DPIA is mandatory or not:

1. evaluation or scoring (including profiling and predicting);
2. automated-decision making with legal or similar significant effect;
3. systematic monitoring;
4. sensitive data;
5. data processed on a large scale;
6. datasets that have been matched or combined;
7. data concerning vulnerable data subjects;
8. innovative use or applying technological or organisational solutions;
9. data transfer across borders outside the EU; and
10. when the processing in of itself 'prevents data subjects from exercising a right or using a service or a contract.'

The WP29 further considers that "[a]s a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA," even though, in some cases, a processing meeting only one of these criteria may require one to be performed.

Concern for companies

Although the WP29 managed to clarify, in most cases, the processing operations that are likely to present a high risk to the rights and freedoms of natural persons (by also including some practical examples of situations where such criteria applies), this topic should still be a matter of concern for companies, as it may be the case that the *ex-ante* determination of a processing as non-threatening proves to be wrong, and the company may in fact

Image: Kyle Spradley / Getty Images

1. 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, WP248 (4 April 2017), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
2. http://www.europeandatacoalition.eu/wp-content/uploads/2015/06/EDC-Recommendation-on-the-GDPR-Implementation.pdf
3. Ibid.

In short, despite the WP29's best efforts to tackle these matters, many questions will persist during the initial application period.

be faced with an operation that requires a DPIA. Hence, the WP29 advises that "if the controller believes that despite the fact that the processing meets at least two criteria, it is considered not to be 'likely high risk,' he has to thoroughly document the reasons for not carrying out a DPIA." At the end of the day, even when the data controller follows all the applicable guidelines when deciding that a processing is not a high risk, while documenting the reasons for its conclusion, it may still be the case that a decision to proceed without a prior DPIA may result in sanctioning proceedings. Controllers must be aware that in the first months and years of application of the GDPR, many of their decisions will not be risk exempt. It will be necessary that that they take into serious consideration the advice given by their data protection officer (should they have one), seek legal advice of specialists on the matter, and pay close attention to the lists published by supervisory authorities regarding the operations that require and do not require a DPIA, as set in Article 35(4) and (5) of the GDPR. When in doubt, to lessen the risk of a wrongful decision, it may be advisable that a controller executes the DPIA, as this will also endorse the idea that the controller is seen as a responsible agent regarding the protection of a natural person's data. Another issue raised by the European Data Coalition is the lack of clarity of the cases in which the controller must consult a supervisory authority, as set in Article 36 of the GDPR, which states that this consultation is mandatory whenever the result of a DPIA indicates that the processing would result in a high risk in the absence of measures to diminish said risk.

As explained by the European Data Coalition, '[I]f the DPIA indicates that the processing would be highly risky, as part of a DPIA the controller [must] introduce appropriate measures to mitigate the risk.' This leaves us with the question of when can the processing 'go ahead without an obligation for prior consultation [if] the controller introduces measures that according to his assessment mitigate this risk?' In attempting to resolve this issue, the WP29 provided an example of an unacceptable high residual risk, in particular, the occurrence of "significant, or even irreversible, consequences" which "[individuals] may not overcome, and/or when it seems obvious that the risk will occur."

The explanation does not seem to be sufficiently clear to eradicate the uncertainty under the GDPR, as the decision of executing a prior consultation is still very much based on the controller's own evaluation, which can be biased, insufficient or wrongfully obtained. Ultimately, this leads to the conclusion that this uncertainty will only and slowly dissipate with the application of the GDPR, which will allow us to see how the supervisory authorities, companies, and, even courts will decide when faced with real life situations. In the long run, the safest position to adopt is, when in doubt, consult.

In short, despite the WP29's best efforts, many questions will persist during the initial application period of the GDPR at least, resulting, potentially, in high costs and high risk-taking by organisations faced with these questions.