26th April 2017

Magda Cocco | mpc@vda.pt
Inês Antas de Barros | iab@vda.pt
Isabel Ornelas | igo@vda.pt
Maria de Lurdes Gonçalves | mlg@vda.pt
Nádia Crujeira da Costa | ncc@vda.pt

PRIVACY, DATA PROTECTION AND CYBER SECURITY

ARTICLE 29 WORKING PARTY GUIDELINES ON THE EU GENERAL DATA PROTECTION REGULATION

In order to clarify some of the new obligations stemming from the EU General Data Protection Regulation ("GDPR"), which will apply as of 25th May 2018, the Article 29 Working Party ("WP29") – the independent European consulting body for data protection issues – recently issued its "Guidance on Data Protection Impact Assessment ("DPIA")". This document will be available for public consultation until 23rd May, 2017.

When is a DPIA mandatory?

The GDPR states that a DPIA (data protection impact assessment) must be carried out when the envisaged data processing operations are "likely to result in high risk to the rights and freedoms of individuals" and sets a list of situations in which the DPIA is mandatory. However, the GDPR stresses that the list is not exhaustive and that, in case of doubt, data controllers must undergo a DPIA. The WP29 also identifies some factors that lead to the performance of a DPIA, such as processing data concerning vulnerable data subjects (minors and employees), the existence of daily data transfers to countries located outside European Union territory, among others.

In case the data controller concludes that a DPIA is not necessary, it must document its analysis and conclusion.

When and how must the DPIA be carried out?

The DPIA is the responsibility of the data controller (which may or not be assisted by third parties) and must be carried out with sufficient advance of the envisaged data processing operations, so that the data controller may address and implement the recommendations arising from the DPIA. The WP29 recommends that DPIAs be reviewed every three years, except when changes are made to the data processing operations. In this case, the reassessment must be made prior to the implementation of such changes.

Which processing operations are subject to a DPIA?

The WP29 clarifies that only data processing operations starting after 25th May 2018 are subject to a DPIA. Data processing operations initiated prior to that date are only subject to a DPIA if the data processing operations are changed following application of the GDPR.

When must the Data Protection Authority be consulted ("Prior consultation")?

The GDPR states that the Data Protection Authority (*Comissão Nacional de Proteção de Dados*, or "CNPD") must be consulted prior to the data processing, whenever the processing would result in high risk, should the data controller's mitigating actions not be implemented. The WP29 also stresses that national law may require data controllers to consult the Data Protection Authority in other situations, even in the absence of such high risk.

Furthermore, following a period of public consultation, the WP 29 approved the final versions of its Guidelines on Data Protection Officers (DPO), the right to data portability (*ie*, the right granting the data subject the possibility, under certain conditions, to receive his/her personal data from the controller to whom he/she had provided those data, as well as the right to transmit those data to another data controller) and on identifying the lead supervisory authority.

Important changes were made to the final versions of the guidelines, among which the following:

1. GUIDELINES ON THE DESIGNATION OF A DPO:

- The designation of a DPO, whether mandatory or voluntary, is made for all data processing activities carried out by the data controller or by the data processor;
- The WP29 recommends that the DPO is based in the EU, even if the data controller or processor are not;
- Even if the DPO is subject to secrecy and confidentiality, he/she may always ask for guidance concerning the data processing carried out by the controller from the Data Protection Authorities;
- Each organisation must have only one DPO, even if he/she is supported by a team;
- Senior Managers, such as the Head of Human Resources, Marketing or IT, may not act as DPO.

2. GUIDELINES ON THE RIGHT TO DATA PORTABILITY:

- Data controllers are not accountable for the data processing operations carried out by the data subject or by the controller to whom the data are transmitted following a data portability request;
- Data processors must assist the controllers in responding to data subjects' portability requests;
- Organizations receiving the personal data are not obliged to accept and process the received data, following a data portability request;
- Personal data related to the data subjects' activity (such as logs or browser search history) are covered by the right to data portability;
- Controllers must explore two complementary ways to ensure data portability: (i) direct transfer of data and (ii) use of an automatic data extraction tool. The choice shall be made in a case-by-case basis.

3. GUIDELINES ON THE LEAD SUPERVISORY AUTHORITY:

- In the event of joint controllership between controllers based in different Member-States, said controllers must find a transparent way to define their respective responsibilities. Moreover, in order to benefit from the one-stop-shop mechanism, they should identify the establishment with the powers to determine the purposes and means of the data processing;
- The one-stop-shop mechanism may also benefit data processors with branches in different Member-States;
- In any event, when several data controllers and processors, located in different Member-States, are involved in the same data processing operation, the lead Supervisory Authority will be the authority in the country where the main establishment of the controller is located – which means that the data processor may have to deal with different supervisory authorities.