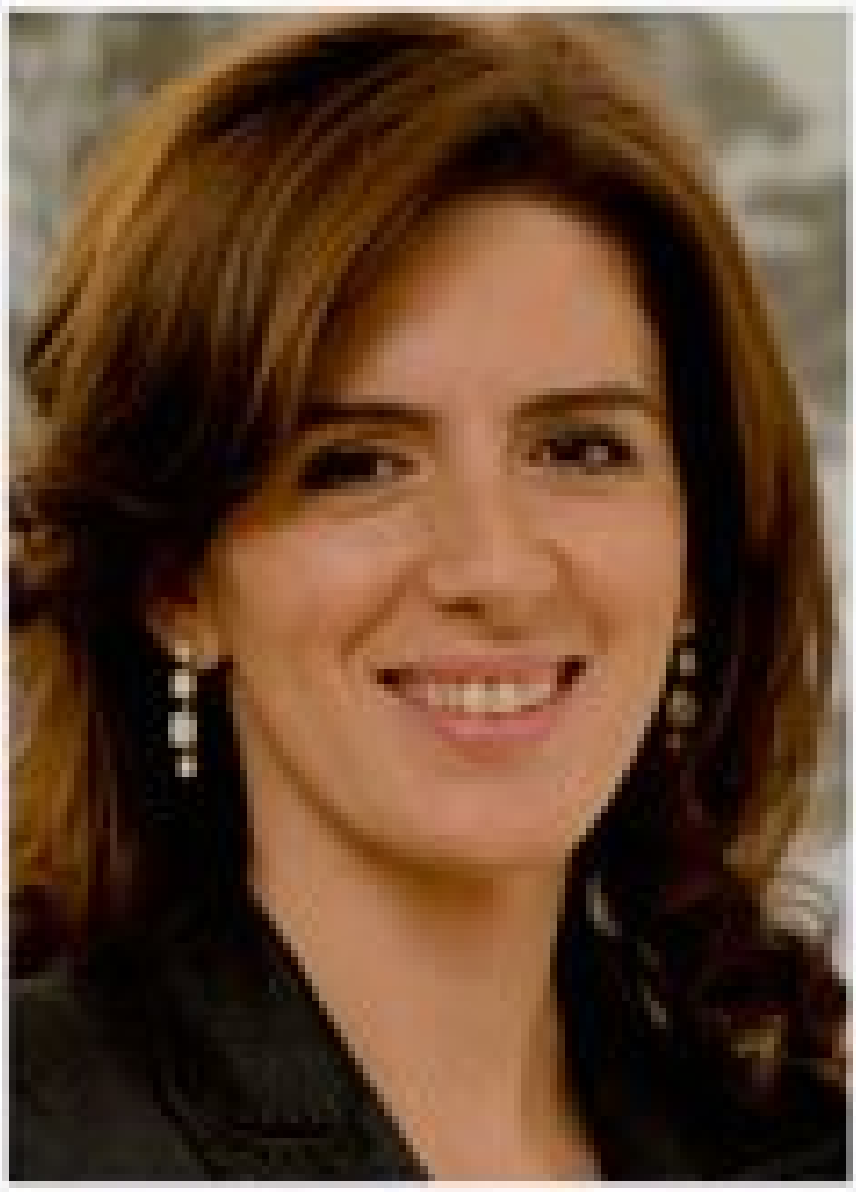
# PREPARING FOR THE GENERAL DATA PROTECTION REGULATION - VDA

*Posted on 21/02/2017*



**Category:** Uncategorized
**Tag:** cat-dataprotection

**On 28 January 2017, the Portuguese Data Protection Authority (*Comissão Nacional de Proteção de Dados*/CNPD) published a document establishing ten measures aimed at helping entities prepare for the application of the General Data Protection Regulation (GDPR). Since the GDPR will apply from 25 May 2018 onwards, the CNPD points out that public and private entities should begin to swiftly implement internal procedures and mechanisms in order to ensure compliance with the new obligations.**

CNPD highlights 10 main areas of intervention, as well as actions to take to ensure compliance. According to the CNPD's guidelines, given the new rules arising from the GDPR, all forms, privacy policies or other texts used to inform data subjects should be reviewed and adjusted to include the additional information required by the GDPR ("right of information").

Whenever applicable, organisations should verify the format, terms and circumstances in which data subject consent was obtained. If not compliant with GDPR rules, a new consent is required ("consent for the processing of data"). Moreover, current internal procedures for replying to data subject requests (including the exercise of new rights, such as the right to portability and the right to be forgotten) should be reviewed so as to ensure compliance with the GDPR's timings and formalities ("exercising data subject rights").

In what concerns the categories of processed personal data, the CNPD advises organisations to evaluate processing operations carried out so as to identify the possible processing of special categories of data and thus determine which criteria should apply ("sensitive data"). Internal policies and practices should be reviewed in order to implement the necessary security measures to ensure an adequate level of security associated with the processing, as required by the GDPR ("technical and organisational security measures"). On the matter of new obligations arising from the GDPR, the CNPD recommends that internal registries of all activities associated with personal data processing should be maintained by data controllers and processors. This is essential for ensuring that both data controllers and processors are able to verify and demonstrate compliance with the GDPR ("documentation and records of processing activities"). It is also necessary to thoroughly assess all projected future processing activities, so as to analyse their nature and context as well as possible risks for data subjects. Organisations will thus guarantee the application of the GDPR principles of data protection by design and by default ("data protection by design and impact assessment").

Organisations should also adopt internal procedures for notifying data breaches. These procedures should include rules and processes regarding the detection, identification and investigation of the circumstances surrounding the breach, mitigating actions, information flows between the controller and the processor, data protection officer involvement and, if applicable, notification to the CNPD and to the data subjects ("security breach notification").

In addition, whenever the GDPR imposes the mandatory appointment of a data protection officer, organisations should ensure its existence beforehand, considering its key role during the implementation of the GDPR. Even when this appointment is not mandatory, the CNPD points out the advantages it has regarding ensuring compliance with the GDPR rules ("data protection officer").

Finally, the guidelines establish that agreements entered into with data processors should be reviewed, so as to include a vast set of information that is mandatory under the GDPR. In the event of subcontracting by the data processors, the latter should not only check existing agreements, but also confirm whether or not this subcontracting was authorised by controllers ("data processing agreements").

CNPD will continue to issue guidelines on the GDPR in line with other European data protection authorities, in order to ensure that it is applied consistently by organisations. Therefore, organisations should consider not only these guidelines and those issued/to be issued by the Article 29 Working Party, but also any future guidelines or recommendations issued by CNPD aimed at preparing for the GDPR.

**Inês Antas de Barros is a managing associate at Vieira de Almeida. She can be contacted at iab@vda.pt**

**Isabel Ornelas is a senior associate at Vieira de Almeida. She can be contacted at igo@vda.pt**

**Maria de Lurdes Gonçalves is an associate at Vieira de Almeida. She can be contacted at mlg@vda.pt**