31 January 2017

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

PRIVACY, DATA PROTECTION & CYBERSECURITY

CNPD APPROVES 10 MEASURES TO PREPARE FOR THE GENERAL DATA PROTECTION REGULATION

On 28th January, 2017, the Portuguese Data Protection Authority (*Comissão Nacional de Proteção de Dados*/CNPD) published a document establishing 10 measures for entities to prepare for the application of the General Data Protection Regulation ("GDPR").

Since the GDPR will apply from 25 May 2018 onwards, CNPD points out that both public and private entities should begin to implement internal procedures and mechanisms so as to ensure compliance with the new data processing obligations.

CNPD highlights 10 main areas of intervention and provides some actions towards ensuring compliance, including the following:

1. **Data subject information:** given the new rules arising from the GDPR, all forms, privacy policies and other informative texts used should be reviewed and adjusted so as to include the additional information required by the GDPR;
2. **Exercising data subject rights**: organisations should review their internal proceedings for replying to data subject requests, including in what concerns the exercise of new rights (such as the right to portability and to be forgotten), so as to ensure compliance with the timings and formalities imposed by the GDPR;
3. **Data subject consent**: organisations should verify the format, terms and circumstances in which data subject consent was obtained. Should this consent not comply with the GDPR rules, new consent is required;
4. **Sensitive data:** it is necessary to evaluate the categories of personal data processed, so as to identify the possible processing of sensitive data (special categories of data, as set out in the GDPR) and thus determine which criteria will apply to this processing;
5. **Documentation and records of processing activities:** the activities associated with personal data processing should be documented, through internal registries of data processing activities and through the implementation of other internal procedures. This is an essential measure towards ensuring that both data controllers and data processors are able to verify and demonstrate compliance with the GDPR;

6. **Data processing agreements:** agreements entered into with data processors should be reviewed, so as to include a vast set of information that the GDPR has deemed to be mandatory. Moreover, 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 the controllers;
7. **Data protection officer:** whenever the GDPR imposes a mandatory appointment of a Data Protection Officer, organisations should ensure its existence beforehand, considering the data privacy officers' key role during the implementation of the GDPR. Even when this appointment is not mandatory, CNPD points out its advantages in what concerns ensuring compliance with the obligations set by the GDPR;
8. **Technical and organisational security measures for processing:** organisations should review all policies, practices and internal measures, in order to ensure an adequate level of security associated with the processing. Organisations should also implement the measures deemed necessary in order to ensure and verify compliance with the GDPR;
9. **Data protection by design and impact assessment:** it is necessary to carry out a thorough assessment of 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 principles of data protection by design and by default, as set out in the GDPR;
10. **Security breach notification:** organisations should adopt and implement internal procedures towards notifying breaches involving personal data. 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 CNPD and to the data subjects.

The organisations which have not yet started implementing the GDPR should, as swiftly as possible, review and adapt their internal proceedings regarding personal data protection, so as to ensure compliance with the GDPR by 25th May 2018.

CNPD will continue to issue guidelines on the GDPR, in order to ensure that it is applied consistently by organisations.

This document is available (solely in Portuguese) at:

- https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf