FEB. 23

INFORMATIVE NOTE

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

CNPD approves guidelines on security measures

On 10 January 2023, the Portuguese data protection authority (Comissão Nacional de Proteção de Dados- "**CNPD**") approved Directive/2023/1[1] ("**Directive**") on organisational and security measures. The purpose of this Directive is to promote awareness among organisations of the importance of implementing appropriate security policies. It makes it clear that the significant number of attacks that occurred in 2022 is mostly due to the lack of investment in this area, which has resulted in vulnerabilities in infrastructures and a lack of user training.

According to the CNPD, the majority of the most frequent attacks affect personal data and result in data breaches that require the application of the provisions of the General Data Protection Regulation ("GDPR") - in other words, *(i)* a risk analysis and documentation of the incident must be carried out, and, depending on this analysis, *(ii)* the CNPD must be notified within 72 hours (the CNPD stresses that this is a continuous period that is not interrupted during weekends and public holidays) and *(iii)* again depending on the risk identified in the first instance, the personal data subjects may have to be notified.

Considering the short period of time to notify the CNPD, the controller should implement internal policies that allow it to detect and manage security incidents with an impact on the protection of personal data. The controller should also ensure effective control mechanisms over the actions of processors to ensure that they do not undermine compliance with its legal obligations.

Taking a preventive approach, the Portuguese data protection authority ("CNPD") aims to combat the increasing number of attacks on information systems, while emphasising that an increasing number of attacks were registered in 2022.

Pedro Lomba
Marta Salgado Areias
Carolina Ventura
Technology, Media and Telecommunications team

1 Available here.

With the publication of the Directive the CNPD aims to make organisations that process personal data - either as processors or as data controllers - aware of the need to invest in this area. The Directive lists some measures by way of example and emphasises that these are necessarily dynamic and should be updated whenever necessary. This updating should be based on the monitoring of the state of the art and the increasing risks. It should also be based on a regular, substantive and in-depth assessment of the processing operations and the impact of the technologies on the functioning of their organisations and, in the case of personal data, on the risks to the rights and freedoms of individuals.

The measures listed in the Directive should be considered by organisations in their prevention and risk mitigation plans. They should also be used as an incentive to strengthen action in this area, as it has become clear that the security measures typically used are no longer sufficient given the level of sophistication of cyber-attacks.

The CNPD recommends, among other things, security audits and vulnerability assessments so that the organisation is aware of its weaknesses. It also suggests the monitoring of the most vulnerable users and consequent investment in training. At an organisational level, the CNPD suggests the implementation of alarm systems that detect situations of access or attempted misuse. These systems will, in turn, allow for faster identification of security incidents.

At the technical level, measures should be adapted to the context. For example, the CNPD recommends the use of systems and infrastructures that allow the segmentation or isolation of data networks to prevent the internal and external spread of malware. Where equipment is used in an external environment, the CNPD stresses in particular that access should only be made via VPN.

The key to implementing appropriate measures lies in tailoring the measures to the specific case and in the dynamism with which they are adapted and reviewed. It is essential to invest in the protection of organisations against increasingly sophisticated cyber-attacks in order to keep pace with the growing level of risk.

In short, the new Directive advocates an alliance between prevention and dynamism. It encourages organisations to define in advance and put into practice prevention plans adapted to the characteristics and sensitivity of the processing of personal data they carry out, as well as to the specific characteristics of the organisation.

Finally, it is important to note that companies and other organisations acting as data controllers under the GDPR are responsible for ensuring that the rights and interests of data subjects are respected, and they must be able to demonstrate that they have put in place the appropriate security measures.

This Directive should be the starting point for organisations to implement appropriate security policies, and to reflect on the growing importance of cybersecurity, as well as the potential damage that a cyber-attack can represent. ■