CUATRECASAS

CNPD Guideline on organizational and security measures

Portuguese National Commission for Data Protection (CNPD) issued several guidelines for data controllers and processors

Portugal - Legal Flash

January 30, 2023

Key aspects

- The National Commission for Data Protection (CNPD) approved its first guideline (Guideline) for 2023 on organizational and security measures for personal data processing.
- The Guideline has been issued in response to increasing attacks on information systems, particularly during 2022,that due to its magnitude and complexity have impacted personal data.
- The attacks are mainly due to (i) infrastructural weaknesses; (ii) users not being trained to detect phishing campaigns; and (iii) data controllers' lack of awareness of the risks to data subjects' rights, caused by the lack of investment in security mechanisms.

Guideline's main points

- Recent years have seen an exponential risein attacks on information systems, which have affected the rights of personal data subjects. In an attempt to promote awareness among data controllers and processors, the CNPD has decided to issue guidelines on their security obligations when processing personal data, these being non-exhaustive, given the pace of technological development.

- The CNPD reinforces the importance of data controllers' obligation to notify the supervisory authority within 72 hours of any personal data breaches that pose a risk to data subjects' rights and freedoms, the obligation to document any data breaches as well as to make data subjects aware of them if there is a risk to those rights and freedoms.

- The CNPD establishes that, for data controllers to safeguard the rights of data subjects, they must first check that all data protection rules are complied with, in line with article 5(1) of the General Data Protection Regulation ("GDPR").

- It clarifies that compliance with data protection rules requires continuous assessments to adapt business or public management models, and technical and organizational resources, given the impact that new technologies have on the way organizations operate and process data.

- The CNPD specifies that organizational and technical security measures must be appropriate to the nature and sensitivity of each type of processing and to the specificities of each organization.

- Regarding organizational measures, the CNPD requires that organizations define and regularly update their incident response plan, classify information according to sensitivity and confidentiality, document security policies, define the best information security practices to be adopted and, among others, promote a culture of information privacy and security among employees.

- Regarding technical measures, the CNPD establishes guidelines on authentication methods that focus on the creation of secure passwords and the implementation of multi-factor authentication.

- Infrastructure and systems must also be updated, organized and designed in a way that enables systems and data networks to be segmented or isolated, while workstation and server security must also be reinforced.

- Similarly, the CNPD stresses the need to define internal policies and procedures on the use of email, the implementation of measures to protect against malware, the way in which paper documents containing

personal data should be stored, and measures regarding the transportation of information that includes personal data.

- The CNPD recommends and encourages data controllers and processors to act in advance, through **preventive and protective measures**, highlighting, in particular, the growing importance of having an incident response plan that takes into account the security measures listed in this Guideline.

Final provisions

Given the importance of this matter, we emphasize the need to:

- implement an **incident response plan** that includes an assessment of the risk to data subjects, ensuring that the controller is able to conclude whether to notify the CNPD of data breaches; and

- adopt **security, organizational and technical measures**, taking into account the nature of the organization and the personal data processing being performed.

For additional information about the contents of this document, please contact your usual *Cuatrecasas* contact.