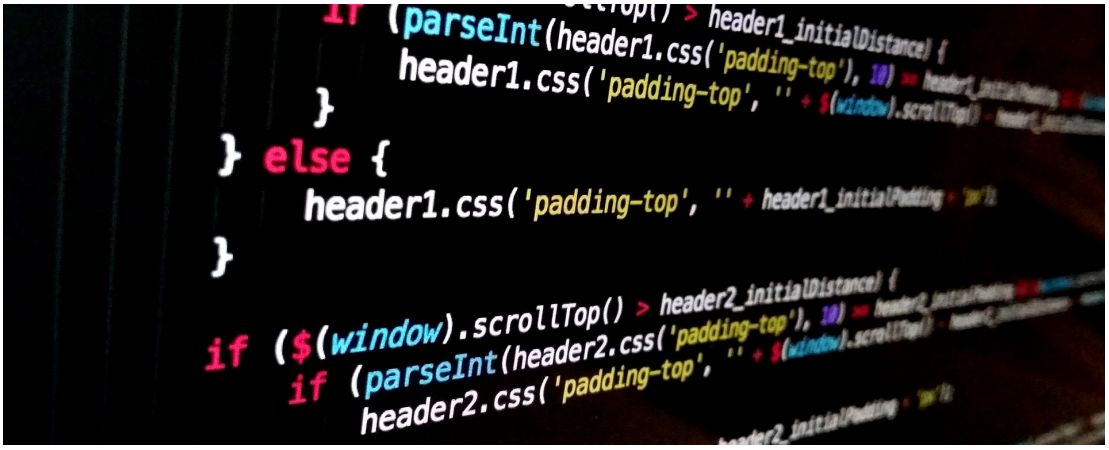
AMMOURA

INSIGHTS



ORGANIZATIONAL AND SAFETY MEASURES IN THE PROCESSING OF PERSONAL DATA: NEW CNPD GUIDELINES

The **National Data Protection Commission** (CNPD) recently published the **Guideline/2023/1** on **organizational and security measures applicable to the processing of personal data** in response to **multiple attacks on information systems**, including phishing, malware and ransomware, occurring with increasing frequency, size and complexity, affecting personal data.

> Entities

Technical and organizational measures shall be adopted, namely, by the **controller** of personal data and the **processor**.

> Technical and organizational measures

Technical and organizational measures aim to provide the processing of personal data with an **adequate level of security for risk**, including the capacity for **confidentiality**, **integrity**, **availability** and **resilience** of processing systems and services.

Examples of organizational security measures:

a) Document **security policies**.

b) Define **secure password management policies**, including size, composition, storage and frequency of change requirements.

c) Create **user management policy**, ensuring access only to necessary data, reviewing the permissions of the various profiles and disabling inactive profiles.

d) Develop **internal policies** to resolve and document **personal data breaches**.

e) Document and fix the identified **security vulnerabilities** without delay.

f) Adopt **alarmist identification** of situations of access, attempts or misuse.

g) Adopt analysis procedures for **monitoring traffic flows** on the network.

h) Conduct **security audits** and **systematic vulnerability assessments**.

i) Promote a culture of **privacy and information security** among employees.

j) Periodically assess and update **internal security measures**.

Examples of technical security measures:

a) **Authentication** — use strong credentials, with long, unique, complex passwords, with numbers, symbols, upper and lower case letters, subject to frequent changes; apply multi-factor authentication.

b) **Infrastructure and systems** — upgrade server operating systems, terminal, applications, and firmware of network equipment; segment or isolate data systems and networks; improve security of jobs and servers by blocking access to sites that could pose a security risk, suspicious redirects through search browsers, and malware-infected files and applications; enable and conserve log audit, validate IP access to servers that are exposed to the public, and configure RDP remote access protocol.

c) **Email tool** — define internal policies and procedures on sending email messages with personal data; encrypt emails and attachments sent with personal data; adopt alarm tool for immediate visibility of creation by users of automatic routing rules to external accounts; implement anti-phishing and anti-spam tools to block maliciously coded links and attachments; adopt security controls to classify and protect sensitive email messages; carry out training actions to enable workers to operate the mechanisms for sending email messages.

d) **Malware protection** — use secure encryption; create system for backups, separated from major databases and without external accessibility; strengthen the system with antimalware tools capable of scanning, detecting and blocking, in real time, threats, including ransomware type.

e) **Use of equipment in an external environment** — set out rules for using equipment; store data on internal systems; allow VPN-only access; block accounts after multiple invalid login attempts; enable multi-factor authentication; apply data encryption to the operating system; enable remote wipe and find my device functions.

f) **Storage of paper documents containing personal data** — use durable paper and printing;

keep documentation indoors, with humidity and temperature control, fire and flood resistant; control access, with record of their date and time, of those who access and the documents accessed; destroy documents by means of specific equipment to ensure safe destruction.

g) **Transport of information containing personal data** — take measures to prevent the unauthorized reading, copying, alteration and deletion of information with personal data; use secure encryption, in transportation, on potentially permanent mass or archive devices, such as CD, DVD, USB PEN.

INSIGHTS

> Notification of personal data breach

A **breach of security** which unlawfully or accidentally causes the destruction, loss, alteration, disclosure or unauthorized access to personal data transmitted, retained or subject to any type of processing must be notified to the CNPD, within a maximum period of 72 hours, where it is likely to result in a risk to the rights and freedoms of natural persons.

Even if **notification to the CNPD** is not required, the controller is obliged to **document** any data breaches under the GDPR.

The controller is also obliged to **inform data subjects** of the occurrence of the data breach, where it is likely to entail a high risk to the rights and freedoms of persons. The main purpose of the notification is to provide specific information about the measures they must take to protect themselves from the negative consequences of the breach of your personal data.

Consequently, the controller should adopt an **internal policy to detect and manage security incidents** with an impact on the protection of personal data and, when the processing of data is carried out by subcontractors, have **effective control mechanisms** as to the actions of subcontractors

Article drawn up in accordance with the legislation in force on 13 March 2023.