On organizational and security measures applicable to the processing of personal data

GUIDELINE/2023/1

1. The attacks on information systems that have been occurring in increasing numbers, especially in the year 2022, some of which are large and complex, affecting, for the most part, personal data.

2. It appears that the main attack vectors have been exploiting the vulnerabilities of infrastructures, the lack of user training to detect phishing campaigns1 that allow then the distribution of malware2, with special relevance to ransomware attacks3, the absence of awareness of those responsible for the treatments regarding the risks to the rights of data subjects data that the lack of investment in security mechanisms entails.

3. In fact, in most of the attacks that were witnessed, the consequences for the rights of holders of the data could have been, if not avoided, at least substantially reduced.

4. Thus, the National Data Protection Commission (hereinafter CNPD), as a supervisory authority national, in pursuit of the attribution defined in paragraph d) of paragraph 1 of article 57 of the General Regulation on Data Protection (GDPR)4, in conjunction with article 3 of Law No. 58/2019, of August 8, understands It is appropriate to make data controllers and processors aware of their obligations under the domain of the security of the processing of personal data.

5. It is alerted to the fact that the security measures for the processing of personal data that are set out below listed are not exhaustive and necessarily dynamic, due to their direct dependence on the technological development and are therefore subject to updating whenever necessary.

1 Phishing is a type of attack that aims to capture sensitive information from a victim, trying to deceive him so that it provides sensitive information, either by clicking on malicious attachments or links in email, or by sharing data in fraudulent pages.

2 Malware refers to any type of program or malicious code created to invade, damage or disable computers and other devices, systems or networks, or even to steal, encrypt or erase data.

3 Ransomware is a specific type of malware that encrypts files stored on servers or computers, making them

inaccessible, and demanding payment for their decryption. Some types of ransomware also extract data from affected computers, sending them to the attackers.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

1v.

I. About Notification of Data Breach

6. A personal data breach is “a breach of security that causes, accidentally or unlawfully, the unauthorized destruction, loss, alteration, disclosure or access to personal data transmitted, preserved or subjected to any other type of treatment», as defined in article 4, paragraph 12) of the GDPR.

7. The RGPD introduces the obligation to notify the personal data breach to the supervisory authority competent national authority, in this case the CNPD, whenever possible, up to 72 hours after becoming aware of the itself, in situations where the violation is likely to result in a risk to the rights and freedoms of natural persons (Cf. article 33.º, n.º 1, of the RGPD).

8. With regard to this period, it is always referred that, even if initially the person responsible for the treatment is not in possession of all the necessary information, it shall notify the supervisory authority without delay, informing that he will later provide the result of the investigation. And it is emphasized that the term is continuous, not suspended on Saturdays, Sundays and holidays.

9. In any case, the information necessary to notify the supervisory authority can be provided by stages, as explained in paragraph 4 of article 33 of the RGPD.

10. Even if the controller considers that notification to the CNPD is not required, he is obliged to to document any data breaches pursuant to Article 33(5) GDPR.

11. The person responsible for the treatment is also obliged to inform the holders of the data of the occurrence of a data breach, if the legal requirements are met and under the conditions described in Article 34. of the GDPR, i.e. "when the data breach is likely to entail a high risk to the rights and freedoms of natural persons', and as soon as reasonably possible. The main objective of this notification is to provide specific information about the measures they should take to protect themselves from

negative consequences of breaching your personal data.

12. It is true that, since 2018, it is primarily up to the person responsible for the processing of personal data ensure respect for the rights and interests of data subjects, with the duty to verify, before carrying out a treatment – as well as the duty to demonstrate – whether all protection rules are complied with of data and whether the specific data processing carried out is in accordance with the principles listed in paragraph 1 of article 5 of the GDPR.

13. In the context of a profound evolution of technology and an increasingly digital economy and society, the achievement of this objective depends on data controllers adapting their models of two business or public management and the respective technical and organizational means to ensure effective compliance with the law and due protection of personal data and the sphere of interests, rights and freedoms of holders thereof.

14. This adaptation should not be merely superficial and formal (bureaucratic), and those responsible for treatment follow the changes of a time that is, in itself, disruptive, through the regular substantive and in-depth assessment of treatment operations and the impact that technologies imply on functioning of their organizations and, in the case of personal data, risks to the rights and freedoms of natural persons.

15. The use of subcontracting does not change the fact that the controller is responsible global protection of personal data. Subcontractors only act on behalf of the person responsible, upon their instructions (cf. Article 4). With regard to the processing of personal data, it imposes the GDPR that their action results strictly from what is prescribed to them by the controller (cf. Article 28(3)(a) GDPR). This is without prejudice to, if the controller gives instructions that violate the GDPR or other provisions of Union or Member State law, the processor must immediately inform the controller of this fact (cf. article 28, paragraph 3, letter h), according to paragraph of the GDPR).

16. Indeed, regardless of the proposals made by the subcontractors, the final decision on the

data processing operations is the responsibility of the controller, who cannot exempt himself from

play its role and comply with its legal obligations, eventually deferring to

subcontractors responsibilities that are yours alone.

17. The controller must have an internal policy in place that allows it to detect and manage

security incidents with an impact on the protection of personal data and, when data processing is

carried out by subcontractors, have effective control mechanisms regarding the performance of subcontractors,

ensuring that those do not jeopardize the fulfillment of the obligations that fall on the person responsible

in this domain.

18. In this context, and in the exercise of its attributions and competences5, the CNPD succinctly defines

guidelines so that data controllers and processors (with the necessary adaptations)

may, through the adoption of appropriate technical and organizational measures, guarantee adequate security

5 Cf. paragraphs b) and d) of paragraph 1 of article 57 and paragraph b) of paragraph 1 of article 58 of the RGPD and articles

3 and 6 of Law no. 8th of

August.

of personal data, including protection against unauthorized or unlawful processing and against loss,

accidental destruction or damage.

II. Technical and organizational measures to be adopted by the controller and the

subcontractor

19. In accordance with the requirements set out in article 32, paragraphs 1 and 2, of the RGPD, it is up to the responsible

responsible for the treatment to evaluate and apply the technical and organizational measures necessary to confer on the

treatment

personal data a level of security appropriate to the risk, including the ability to guarantee the

confidentiality, integrity, availability and resilience of treatment systems and services.

20. In this sense, and depending on what is appropriate to the characteristics and sensitivity of each treatment of

personal data carried out and the specificities of the specific organization, the following should be considered

security measures:

A. Organizational

The. Define and regularly exercise the incident response and disaster recovery plan,

providing the necessary mechanisms to guarantee the security of information and the resilience of

systems and services, as well as ensuring that data availability is restored

in a timely manner after an incident;

B. Classify the information according to the level of confidentiality and sensitivity and adopt the

organizational measures and techniques suitable for classification;

w. Document security policies;

d. Adopt analysis procedures for monitoring traffic flows on the network;

It is. Define strong password management policies, imposing requirements for length,

composition, storage and how often a password needs to be changed;

f. Create a user lifecycle management policy to ensure that each worker

has access only to the data necessary to perform its functions and review frequently

the permissions of the various user profiles, if possible, as well as the deactivation/revocation of

inactive profiles

g. Adopt an alarm system that allows identifying situations of access, attempts or misuse;

H. Define, in an initial phase, the best information security practices to be adopted, either in the

software development, or in the acceptance testing phase, considering in particular:

data protection principles by design and by default, risk analysis of processing

and data lifecycle, data pseudonymization and anonymization methods – even

when the system is developed and maintained by subcontractor(s);

i. Perform IT6 security audits and vulnerability assessments (penetration testing)

systematic, so that users can be aware of their weaknesses and to

that organizations manage to monitor the most fragile targets and invest in training with

specific and targeted content, according to the vulnerabilities detected;

j. Verify that the defined security measures are in place, ensuring that they are effective and

updating them regularly, especially when processing or circumstances become

change, including those implemented by subcontractors in data processing;

k. Document and correct detected security vulnerabilities without delay;

l. Take the necessary measures to ensure full compliance with article 33 of the GDPR, in

particularly with regard to the development of an internal policy for dealing with and documenting

possible violations of personal data;

m. Foster a culture of privacy and information security among employees, so that

each employee is able to recognize potential threats and act accordingly,

and as a way to reduce the occurrence and impact of human error;

n. Make employees aware of the duty of confidentiality to which they are subject due to the fact that

process personal data;

O. Periodically evaluate internal security, technical and organizational measures and carry out the

its updating and revision whenever necessary.

B. Techniques

i. Authentication

The. Use strong credentials with long (at least 12 characters), unique, passwords

complex and with numbers, symbols, uppercase and lowercase letters, changing them frequently;

B. Equate, namely in view of the sensitivity of the information, the privileges of users or

the form of access (eg remote), the application of multifactor authentication;

6 Information Technologies.

3v.

ii. Infrastructure and systems

The. Ensure that server and terminal operating systems are up to date, as well as

all applications (eg browser and plugins);

B. Keep the firmware of network equipment updated;

w. Design and organize systems and infrastructure in order to segment or isolate systems and

data networks to prevent the spread of malware within the organization and to systems

external;

d. Strengthen the security of workstations and servers, namely:

i. block access to sites that are likely to pose a security risk;

ii. block suspicious redirects via search engines;

iii. immediately block files and applications infected with malware2;

iv. perform periodic inspection of the status and use of system resources;

v. monitor usage of installed software;

saw. activate and maintain audit records (log);

vii. validate IP accesses to servers that are exposed to the public;

viii. change the port configured by default for remote access protocol (RDP).

iii. email tool

The. Clearly and unequivocally define internal policies and procedures on the specific sending of

email messages containing personal data, which introduce the checks

additional necessary, in the sense of:

i. ensure that recipients' email addresses are entered in the 'Bcc:' field,

in cases of multiple recipients;

ii. prevent errors in manually entering email addresses;

iii. ensure that the attached files contain only the personal data that is

intend to communicate;

B. Equate the creation of distribution lists or contact groups, with the aim of preventing the

disclosure of recipients' addresses in mass mailing operations

e-mail;

w. Equate the creation of rules with the objective of postponing/delaying the delivery of mail messages

electronic file containing personal data, keeping them in the 'Outbox' for a certain time,

allowing compliance checks after clicking 'Submit';

d. Encrypt with a code, to which only the recipient has access, the emails and/or attachments sent that

contain personal data;

It is. Confirm with the recipient, before sending an email containing personal data, the email address

preferred email for contact;

f. Carry out training actions in order to enable workers to operate the mechanisms of

sending email messages in accordance with the defined procedures,

sensitizing them to the most common errors, potentially susceptible to originating violations of

personal data and encouraging them to double check;

g. Reinforce the alert system of the alarm tool used by the entity, to ensure

immediate visibility into user creation of automatic email routing rules

emails to external accounts;

H. Reinforce the system with anti-phishing and anti-spam tools, which allow blocking calls and/or

attachments with malicious code;

i. Adopt security controls that allow classifying and protecting mail messages

sensitive electronics.

iv. malware protection

The. Use secure encryption especially in the case of access credentials, special data7,

data of a highly personal8 nature or financial data;

B. Create an up-to-date, secure, and fully tested backup system

separated from the main databases and without external accessibility;

7 The personal data listed in paragraph 1 of article 9 of the RGPD.

8 Roughly speaking, personal data related to criminal convictions and offenses (cf. article 10 of the RGPD) or with dimensions

of private and family life.

4v.

w. Reinforcing the system with anti-malware tools that include the ability to scan and detect it,

as well as real-time blocking of ransomware-type threats.

v. Use of equipment outdoors

The. Store data on internal systems, protected with appropriate security measures, and

remotely accessible via secure access mechanisms (VPN);

B. Allow access only via VPN;

w. Block accounts after multiple invalid login attempts;

d. Enable multifactor authentication for device users;

It is. Apply data encryption in the operating system;

f. Whenever applicable, activate the “remote wipe” and “find my device” functionality;

g. Automatically back up work folders when the device is turned off

is connected to the entity's network;

H. Define clear and appropriate rules for the use of equipment in an external environment.

saw. Storage of paper documents containing personal data

The. Use paper and printing that is durable;

B. Keep documentation in a place with humidity and temperature control;

w. Store, properly organized, documents containing sensitive personal data in

closed place, resistant to fire and flood;

d. Controlling access, with registration of the respective date and time, who accesses and the specific(s)

document(s) accessed.

It is. Destroy documents using specific equipment that guarantees “safe” destruction;

vii. Transport of information that includes personal data

The. Adopt measures to prevent that, in the transport of information with personal data, these may

be read, copied, altered or disposed of in an unauthorized manner;

B. Use secure encryption in transport, on potentially mass or archival devices

permanent (CD/DVD/USB PEN).

III. Conclusion

21. Controllers and processors are encouraged to define in advance and

put prevention plans in place so they can protect their systems and infrastructure and have

mechanisms ready to detect a breach of personal data and quickly mitigate the negative effects

on the rights of the respective holders. This incident response plan should include an assessment of the

risk for these natural persons, which allows the controller to conclude whether to notify the

data breach, both to the supervisory authority and to the affected data subjects.

22. The information needed to notify the supervisory authority can be provided in stages, but this does not

excludes the obligation for the controller to act in a timely manner to respond to the data breach

personal.

23. Thus, pursuant to article 57, paragraph 1, point d) of the RGPD, the CNPD recommends that the person responsible for the

treatment, as well as the subcontractor (with the necessary adaptations), to adopt security measures

listed in this guideline, depending on what is appropriate to the characteristics and sensitivity of the

processing of personal data carried out and the specificities of its organization, with a view to giving

compliance with the obligations provided for in article 32.º, paragraphs 1 and 2, of the RGPD, regarding the security of the treatment

of personal data.

Approved at the CNPD meeting on January 10, 2023