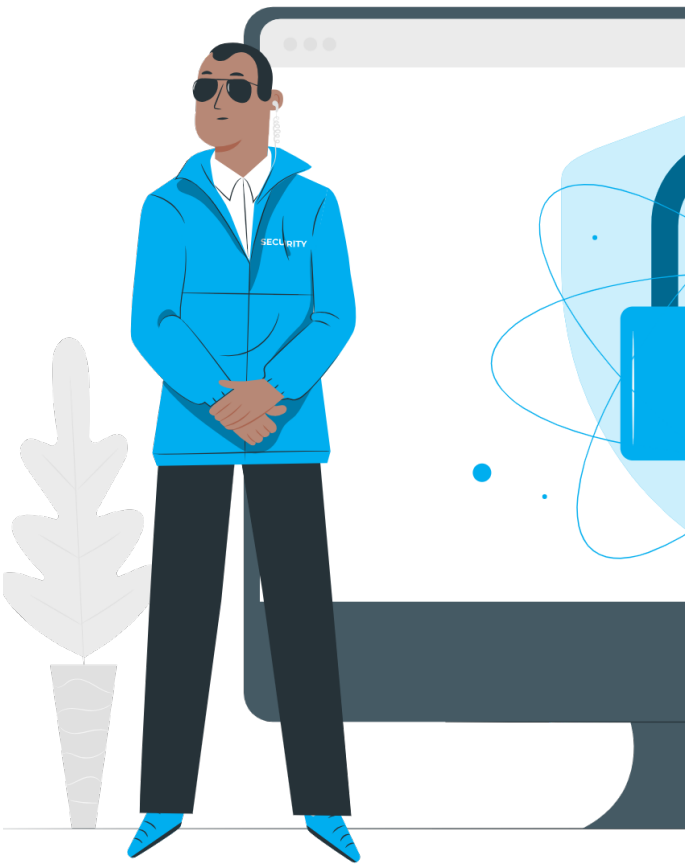
Factsheet 9:
Security, technical and organisational measures (Art. 32)



Responsibilities of the controller

The organisation that is the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This includes means that can ensure the confidentiality, integrity and availability of the IT systems in place. It must also implement means to restore the availability of personal data in the event of an incident (Article 32 GDPR).

In the event of a personal data breach, the controller is required by Article 33 GDPR to notify the CNPD. The data breach notification form can be downloaded from the CNPD website and sent to the email address databreach@cnpd.lu.

How to prevent the success of an attack?

Illustration of the technical and organizational measures to be put in place to reduce the risk of ransomware:

- **Raising user awareness:** Human error remains a major factor in data breaches. Most often, the ransomware attack starts with opening a booby-trapped attachment or viewing a malicious webpage. Thus, training users in good digital security practices is a fundamental step to combat this threat.
- **Create a dedicated contact point:** Dedicate one or more persons that users of the IT system are obliged to notify in case of suspicion of a security incident. This contact point must be reachable at all times and each user must know how to contact him.
- **Require strong and unique passwords:** All user accounts must be protected by strong and unique passwords. Two-factor authentication (2FA) is also recommended, especially for external access as well as for access to critical machines of the IT environment (e.g. domain controllers).

Update : 4th June 2024

Factsheet 9:
Security, technical and organisational measures (Art. 32)

- **Save data:** Regular backups of all data, including those on critical file, infrastructure and business application servers, shall be performed. These backups, at least for the most critical ones, must be disconnected from the information system to prevent their encryption, like other files. The use of cold storage solutions, such as external hard drives or magnetic tapes, protects backups from system infection and keeps data critical to recovery.

- **Keep software and systems up to date:** Unpatched vulnerabilities of operating systems or software present on the information system may be used to infect the system or promote the spread of infection. It is crucial to install the available updates (including security patches) as soon as possible.

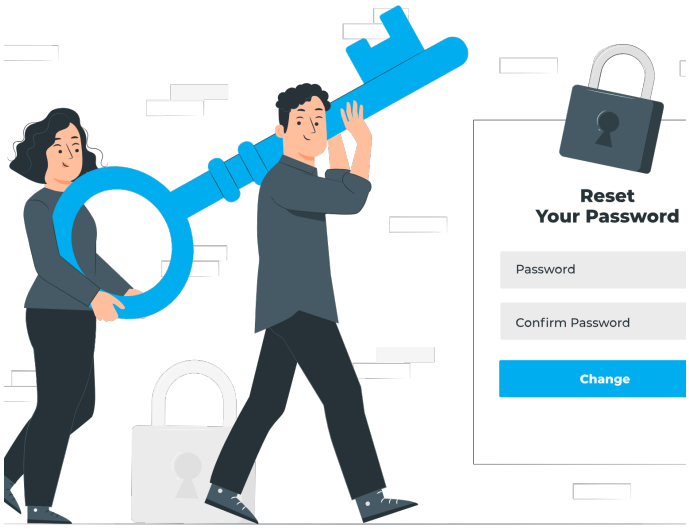
- **Use and maintain antivirus software:** Although antiviruses do not guarantee protection against as yet unknown ransomware, the use of these tools is still necessary on exposed resources (workstations, file servers, etc.). For these tools to be effective, it is important to perform frequent updates and regularly ensure that there is no known malware on the entity's file storage spaces.

- **Segmentation of the information system:** Without a protective measure and from a single infected machine, ransomware can spread across your entire information system and infect most accessible machines. In order to limit the risk of spread, the information system should be segmented into zones each with a homogeneous level of security (e.g. internal server area, internet exposed server area, user workstation area, administration area, etc.).

- **Limit user rights and application permissions:** Users must not be administrators of their workstation. This limits the possibility of software installation and unintentional execution of malicious code. In addition, a regular review of these users and their rights must be carried out in order to ensure that this corresponds to the reality of the organisation's needs (employee departures, job changes, etc.).

- **Set up encryption software:** Implementing encryption technologies is an additional security measure to protect your stored data. As a result, even if criminals succeed in stealing your data, they will not be able to access or disclose it (provided that the encryption/decryption keys are not compromised).

- **Reinforcing IT security in teleworking:** If your company's employees are entitled to telework, it's essential to keep professional and personal tools separate. If your company has set up a computer with secure access, firewalls and other antivirus, only this equipment should be used. Employees must also communicate exclusively via secure business messaging and enter a digital teleworking space protected by a strong password and/or dual authentication. Setting up VPN network tools for business flows makes it possible to secure exchanges and prevents a personal computer from becoming a collision gateway for hackers.



Factsheet 9:
Security, technical and organisational measures (Art. 32)

- **Prepare a crisis communication plan:** In the event of a ransomware attack, your email and phone infrastructure may be disrupted. It is therefore necessary to prepare offline communication channels. Keep printed copies of essential mobile phone numbers (computer suppliers, support teams, etc.)

- **Consult the CIRCL MISP platform:** CIRCL (Computer Incident Response Center Luxembourg) offers the possibility for a private organization to connect to MISP («Malware Information Sharing Platform»), a platform for sharing information about existing malware and threats. The objective of MISP is to improve the countermeasures used against targeted attacks and to implement preventive and detection actions.