Technical and organizational measures according to Art. 32 GDPR

Conundra BV

Safety concept

Technical and organizational measures according to Art. 32 GDPR

Basic measures

Fundamental measures that serve to safeguard the rights of data subjects, respond immediately in emergencies, meet the requirements of technology design, and protect data at the employee level:

- Employees are obligated to maintain confidentiality with regard to data protection, are instructed and briefed, and are made aware of possible liability consequences. If employees work outside the company's internal premises or use private devices for business activities, special regulations exist to protect data in these constellations and to safeguard the rights of clients of commissioned processing.
  Confidentiality for employees is ensured by Data Classification policy.
  Rules for secure teleworking (clean desk & clear screen) are listed in IT Security policy.
  Liability consequences are communicated to all employees by HR with the disciplinary clause.

- There is an internal data protection management system, compliance with which is constantly monitored and evaluated as required and at least annually.
  An annual penetration test, internal audit and external audit review is performed.

- Keys, access cards or codes issued to employees, as well as authorizations granted with regard to the processing of personal data, shall be withdrawn or revoked after their departure from the company or change of responsibilities.
  There is an onboarding/offboarding process in place and a process for regular review of user access rights.

- The software used is always kept up to date, as are virus scanners and firewalls.
- The cleaning staff, security guards and other service providers used to perform ancillary tasks are carefully selected and it is ensured that they observe the protection of personal data.
- Clean desk policy to ensure that unaccompanied external service providers do not have access to personal data.

Entry control

- Security locks
- The front door is locked with key and security code.
- Access regulations for persons outside the company
  There is a policy for non-accompanied service providers.

- Window lock instruction
  Windows shall be locked by the last person leaving the building.

- Supervision of auxiliary staff
  All external visitors are accompanied.
  If they are not accompanied (e.g. cleaning staff), they sign a specific document.

Access control

- Use of VPN technology
- Encryption of mobile devices (laptops)
- Minimum password lengths and password managers
- Authorization/authentication concepts with access regulations limited to the most necessary
- Always current software versions
- Always up-to-date virus protection
- Use of intrusion detection systems
  Microsoft defender.

- Authentication with user and password and, in the case of increased protection requirements, by additional multifactor authentication
- Logging of accesses to data
- Guideline for the use of USB sticks
  There is a policy that forbids use of USB sticks.

- Encryption of hard disks (FileVault, Bitlocker)
- Proper destruction of data carriers
  There is a procedure for erasing laptops.

Transfer control

- Encryption of data carriers and connections
- Determination and documentation of the recipients
  There is a data classification procedure.

Input control

- Assignment of rights to enter, change and delete data on the basis of an authorization concept
  There is an access control policy.

- Retention of forms from which data have been transferred to automated processing operations
  For OptiFlow downloads.

Order control

- Control of compliance with contractors
  The requirements are specified in the contract and in the confidentiality agreement.

- Ensuring the destruction of data after the completion of the order
  Either PC is enrolled and managed with controlled on and off boarding, or there is access to the web version, which can be revoked.

Availability control / integrity

- Additional backup copies with storage in specially protected locations
- Constantly controlled backup and recovery concept
  Database can be restored to a specific point in time.

- Uninterruptible power supply and surge protection
- Carrying out resilience tests
  There is an early disaster recovery procedure test.

Guarantee of the earmarking/separation requirement

- Logical client separation (software)
- Separation of productive and test system