Technical and Organisational measures

Data protection and data security concept

This document provides a summary of the technical and organisation measures deployed across the business as per Art. 24(1) of the EU General Data Protection Regulation (GDPR) for commissioned data processing.

The effectiveness of the measures take into account the protection objectives of confidentiality, availability, integrity and capacity. This is supported by integrating data protection measures, informational security and additional measures to safeguard data processing operations.

Definition of security value terms:

Confidentiality: Protection of data, information and programmes against unauthorised access and disclosure

Integrity: Factual and technical accuracy and completeness of all information and data during processing

Availability: Information, data, applications, IT systems and IT neworks are available for processing

Resilience: Denoted as an aspect of availability and thus the capacity of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

Confidentiality

essensys implements physical and logical access controls across its networks, IT systems and services to provide authorised, granular, auditable and appropriate user access and to ensure appropriate preservation of data confidentiality, integrity and availability.

a. Physical Access control
   Measures are implemented that deny unauthorised persons access to data processing system that process and/or use personal data. This is done by:

    a. Data Centre / Servers
       Access to data centres is restricted to named personnel only.
       Government ID is required on entry to the 24/7 manned reception.
       Video surveillance at entrances/exits,
       Security gates required to access secure server rooms
       Secure, dedicated cages used to host server infrastructure

    b. Office Administration
       Physical access to essensys offices, where restricted, is controlled primarily via Card, Key fob or Smart Access account.
       24-hour CCTV on entrance and exits
       Segregated Comms room with restricted access

b. Device / Systems Access control
    a. Personal User IDs are allocated
    b. Use of secure complex passwords
    c. Multi-factor authorisation enforced
    d. Centralised user administration
    e. Access authorisation is granted to users based on authorisation procedures
    f. Users can only have access to personal data according to the authorisation granted to them (by means of role allocation, functional user, etc.)
    g. VPN required to access internal network devices (when working remotely)

c. Separation control
    a. Customer data is logically separated from other customer data
    b. Data is backed up on logically and physically separate systems
    c. There is a separate logical network for office visitors

Integrity

Factual and technical accuracy and completeness of all information and data during the processing of personal data are guaranteed. The identification and correction of unauthorised modifications must be ensured. The following checks ensure the integrity of personal data:

a. Transfer and cryptographic controls
    a. Data transfer takes place in protected networks
    b. Use of information encryption to protect sensitive or critical information, either stored or transmitted
    c. Use digital signature certificates or message authentication codes to verify authenticity or integrity of stored or transmitted sensitive or critical information (HTTPS/SSL/TLS)
    d. Filter mechanisms prevent connections to/from unauthorised systems (firewall)
    e. Data is deleted in compliance with data protection regulations after termination of contract or at the request of the customer

b. Input / Storage Control
    a. Storage or personal data on removable media is not permitted
    b. Personal data are exclusively stored and held on data storage devices in a central data centre with secured access
    c. Data storage devices are disposed of in accordance with data protection requirements and destroyed by a 3rd party disposal firm

Availability and resilience

It should be guaranteed that personal data are protected against the risk of accidental destruction or loss. To this end, the following measures have been implemented:

a. Availability control
    a. Built-in redundancy across systems by design
    b. Backup and recovery procedures in place for all critical systems.
    c. Implementation of protection programs
    (virus scanners, firewalls, spam filters)
    d. Monitoring of all relevant devices
    (network, servers, application)
    e. Permanently active DDoS protection and bandwidth monitoring
    f. 24/7 Network Operations team
    g. Use of uninterruptible power supplies
    h. A Disaster Recovery / Business Continuity Plan has been prepared and is reviewed and tested annually

b. Threat and Vulnerability
    Numerous controls are in place to mitigate threat and vulnerability risks. A summary of the controls is listed below;

        a. Layered network defence

b. Protective monitoring
c. Client anti-malware
d. Server anti-malware
e. Use of external vulnerability assessment
f. Software versions
g. Client patching
h. Server patching
i. Application patching
j. Firmware patching

Procedures for regular review, assessment and evaluation

The effectiveness of the measures implemented must be reviewed, assessed and evaluated by means of internal processes and procedures, especially at organisational level.

- Data Protection policy established
- Incident Response policy in place
- Data protection by design and by default
- Process in place to ensure written contract exists between customer and data processor
- Sufficient measures taken to ensure compliance with data protection by a possible sub-processor
- Monthly internal audits
- Monthly security meetings
- Process in place for onboarding staff
- Process in place for offboarding staff
- Reviews of data protection and security standards
- External audits of policies and procedures to maintain ISO27001 and SOC2 accreditations