7 Maintenance (operation)

This checklist is dynamic, not exhaustive, and will be updated regularly. If you have any suggestions or comments, we would like to hear from you.

How to handle incidents and data breaches?

- Implement and operate a plan for incident response management (prepared during the release activity).
- Security incidents must be given high priority.
- Handle incidents and data breaches:
  - Detect abnormal activity, traffic, security incidents, and data breaches.
  - Analyse/Verify whether abnormal activity, traffic, security incidents, and data breaches are actual security breaches or false positives
  - Report security breaches and data breaches according to internal guidelines for incident response handling.
  - Handle security incidents and data breaches according to the organisation’s continuity plan for restoring the normal state of maintenance, service and operation.
- Incident response training covering unexpected scenarios should be done periodically.

Maintenance, service and operation

- Identify and allocate roles, responsibilities, and authority.
- Handle the data subjects’ rights and request related to this, such as data access, modification, deletion, data portability, consent, information, transparency, etc.
- Continuously assess the effectiveness of technical and organisational security measures for uncovering vulnerabilities.

Examples:

- security tests (such as vulnerability analysis and penetration testing, continuous automated health checks of software, infrastructure and network).
- training (such as topic- and industry-specific drills, desktop, games, etc.)
- testing and measurement of the security culture (such as campaigns, surveys to be answered, etc.)

- Metrics comparing the effect of security measures to their intended purpose.
- Data, platform, network, and software maintenance includes:
  - identifying and monitoring potential points of attack, such as applications, servers, networks, endpoints, etc.
  - error debugging, updating and patching of server and client software and third-party components
  - performance improvements
  - logging of system events and user activity for security checks
  - periodic reviews of logs to uncover security breaches
- correction, deletion, and phasing out of data and applications, such as developers with oversight over the entire production process, and who continuously implement measures to improve IT solution
- upgrading and phasing out of software libraries
- tackling new security challenges and handling new vulnerabilities
- updating and maintaining crypto algorithms and keys

- Update contingency and continuity plans.
- Conduct periodically training of the plans
- Conduct regular internal and external audits, to document compliance with regulations, and to eliminate data breaches.
- Periodically audit data processors using the data processing agreement and relevant auditing criteria, such as legislation, codes of conduct, internal regulations, and security frameworks.
- Check and review user’s and supplier’s access.
- Perform regular risk and vulnerability analyses, based on earlier risk and vulnerability analyses.
- Conduct data protection impact assessments when significant changes, or development of, software occurs.
- Establish and present the current status of privacy and security to the management.

**Why impose requirements for maintenance, service and operation?**
- The data controller must have a full record of processing activities relating to personal data, and data processors must keep a similar record of their actions on behalf of different data controllers, cf. Article 30.
- There are security requirements for the processing of personal data, cf. Article 32.
- There are requirements for data protection by design and by default in solutions, programs, apps, and systems that manage personal data, cf. Article 25.
- There are requirements for a data protection impact assessment upon start up or for significant changes relating to the processing of personal data, cf. Article 35.
- There are requirements to ensure the data subject’s rights, cf. articles 12-23.
- There are requirements to ensure compliance with the privacy principles, cf. Article 5.
- Secure maintenance, service and operation are anchored in the organisation’s management.
- The data controller is required to make use of data processors who are bound by the General Data Protection Regulations, cf. Article 28.