1 Training

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

What training should be provided?

Training should be given in the following topics:

- The General Data Protection Regulation in general, particularly following themes;
  - principles of privacy, Article 5
  - the lawfulness of processing, Article 6
  - conditions for consent, Articles 7 and 8
  - processing of special categories of personal data, and criminal offences, articles 9 and 10
  - Chapter III concerning data subjects' rights, Articles 12-23
  - Chapter IV on the duties of data controllers and data handlers, Articles 24-43, particularly
    - privacy by design, and privacy by default
    - records of data processing activity
    - security of personal data
    - notification of personal data and information security breaches to the supervisory authority, and notification of data breach to the data subject
    - data protection impact assessment and prior consultation
    - data protection officer, appointment, job descriptions, overview of tasks
    - codes of conduct and certification
- laws and regulations related to the subject area of the software to be developed (e.g. patient record law, Privacy and Electronic Communications Regulation (ePrivacy), ICT regulation)
- mandatory business / sector / industry requirements and code of conduct
- the organisation's own information security requirements and guidelines
- the organisation's own internal security protocols
- roles and organization in the organisation relating to privacy and information security
- Information Security Framework (e.g. ISO27001, Standard of Good Practice (SoGP))
- Framework for software development (e.g. Microsoft Security Development Lifecycle (SDL), ISO27034
- security testing (e.g. OWASP Top 10, OWASP Testing Guide, OWASP ASVS walkthrough)
- threat and risk assessment (e.g. STRIDE, DREAD, Microsoft Threat Modelling Tool) documentation requirements

Who should receive training?

- All employees should have a basic understanding of privacy and information security.

- Management should be competent in how to assess the impact and consequence of privacy implications, risk assessment, the responsibilities of management, and handling of risks relating to privacy and information security.
- Project leaders should be competent in the topics of data protection by design and by default and information security by design.
- Developers should be competent in the topics of secure coding, and privacy and security by design.
- Architects should be competent in the topics of secure architecture, data protection by design and by default and security by design.
- Testers should be competent in the topics of security testing, data protection by design and by default and security by design.
- Suppliers should be competent in the topics of secure maintenance, service and operation, data protection by design and by default and security measures, data processing agreements, incident response handling, and emergency response. The suppliers should have readable, standardized and updated security documentation to be in compliance with GDPR.

When training should be given?

- at the start of employment
- with updates at regular intervals
- at the start of a (development) project

Example on how training should be carried out:

- through differentiated education programs at different detail levels, ranging from the basic skills (minimum mandatory skills) to specialised and/or in-depth knowledge (this can be for dedicated employees)
- using different educational techniques and tools (such as classroom training, course materials, workshops, e-learning, competitions, one-on-one discussion, certifications, courses, metaphors (easy-to-remember cartoon shorts such as "bobby tables" for example https://xkcd.com/327/), one-pagers, movies, rewards, etc.
- by updating employees based on results from internal assessments
- by updating employees based on results from penetration testing and vulnerability assessments
- by ensuring that employees familiarise themselves with the organisation's policies for privacy and information security policy, including the data protection by design and by default requirements
- as a regular fixed point on the agenda in developer forums and industry conferences.

Why training should be carried out?

- The General Data Protection Regulation requires that appropriate technical and organizational measures are taken to safeguard the rights and freedoms of natural persons and particular their right to the protection of personal data. Training is an organizational measure, and is a duty reflected in the General Data Protection Regulation, Articles 24, 25, 28, 32, and 39 (1) b).
- The training must have the support of management, and accordingly the organization.