2 Requirements

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.

Requirements for software, products, applications, systems, solutions, or services must:

- fulfil the data-protection principles
- protect the data protection rights of the data subject
- fulfil the company's obligations
- ensure that that settings are by default set to the most privacy-friendly option
- ensure that the end product is robust, secure, and provides enforceability of the data subjects rights

What needs to be done before the requirements are set?

- Define the processing to be done, and establish an overview of the personal data:
  - Will personal data be processed by the software?
  - Identify the controller, and any processors and subcontractors. Processing contracts must be signed, and subcontractors must be approved by the controller.
  - What is the legal basis for the processing?
  - What is the purpose of the processing?
  - For how long does the legal basis and/or the purpose allow storage of personal data? Is it necessary to plan for automatic erasure?
  - Define the categories of personal data that is *necessary* to be processed to achieve the purpose. The processing of special categories of personal data and personal data relating to criminal convictions and offences (sensitive personal data), is generally prohibited, with some exceptions, so determine if one of these exceptions will apply. Document the full scope of data stored within the software.
  - How is transparency being achieved? Automatic notifications by the system, privacy dashboard, etc.?
  - Is personal data being transferred to a third country, or to an international organisation? Conditions apply to the transfer of personal data to third countries or international organisations, including restrictions on access, operations and storage. Where personal data is to be transferred to a third country or an international organisation, it is important to ensure that all such transfers are lawful.
- In what context will the processing take place? Is it likely that the software could be used in another context?
- Identify all requirements that apply to your business: Are there codes of conducts specific to the industry or sector? Are there any policies and requirements that can help you determine requirements for the software?
- Are there certification schemes you can, and should, aim to follow? What requirements apply in such cases?

- Has the Data Protection Authority made any administrative decisions in this field, relating to your own business or to other comparable businesses, that should be included as requirements in the software?

Requirements for data protection and information security

- If the software is working as intended without identifiable data, no identifying data must be collected.
- Data protection can be designed in using pseudonymisation techniques in the software.
    - Unnecessary identification and redundant personal data in the software result in greater risk to the user or the data subject. It also makes the software more vulnerable and attractive to actors wishing to reuse the data for other purposes.
    - The software must only use personal data as planned, and all data must be deleted when storage is no longer lawful according to the legal basis or no longer necessary to fulfil purpose.
    - Personal data must be available to those authorised to use it when necessary.
    - The software must be developed with default settings that protect the rights of data subjects and safeguards privacy.
    - The software should guide the user to the most privacy-friendly manner of use. For example, location sharing should be disabled by default, with the user able to activate it if required.

Requirements for meeting data-protection principles

The basic requirements for software being used to process personal data are:

- Lawfulness, fairness, and transparency
    - Processing of personal data in the software is only lawful if one of the following applies:
        - the data subject has given her/his consent
        - the processing is necessary for the performance of a written agreement or contract with the data subject
        - the processing is necessary for compliance of a legal obligation
        - the processing is necessary to protect vital interests of the data subject or another natural person
        - the processing is necessary to perform a task carried out in the public interest or in the exercise of official authority
        - the processing is necessary for the purposes of legitimate interests pursued by the controller (balancing of interests)
    - The software must ensure default settings that protect the rights of data subjects and safeguards privacy.
    - Processing of personal data must be predictable by the data subject, and performed with respect for the data subject's interests.
    - The software must be designed in a way that relevant aspects of personal data processing are known to the data subject, so that the persons concerned can make informed decisions or exercise their rights
    - The software must ensure that other rights, such as freedom of expression, freedom of thought, absence of discrimination and freedom of religion, are safeguarded.

    - Clear and comprehensible information must be provided to the data subject regarding the purpose of the processing of personal data, the legal basis, recipients of the information
- purpose limitation
    - The software must only collect personal data for specified, explicit and legitimate purposes.
    - The personal data must not be further processed in a manner that is incompatible with the original purposes.
- data minimisation
    - The software must only process personal data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy
    - The software must ensure that all personal data is accurate and up-to-date. Incorrect data must be deleted or rectified.
- storage limitation
    - The software must ensure that it is not possible to identify the data subject for longer than is strictly necessary for the purposes for which the personal data are processed.
- integrity and confidentiality
    - The software must ensure appropriate security of the personal data.

If the software operates based on **consent:**

- The consent must be explicit (not passive), voluntary (no coercion/pressure), and informed (predictable).
- The processing that is based on consent shall be clearly distinguished from other matters
- A declaration of consent must be written in clear and plain language at the reader's level, and be intelligible and easily accessible to the user. Separate conditions apply to children's use of information society services.
- The users must be able to withdraw consent at any time and as easily as they give it.

Requirements to protect the rights of the data subject

The obligation **to provide information** differs depending on whether the personal data is obtained from the data subject or if it is obtained directly from a system or from persons other than the data subject.

When personal data is obtained from the data subject, he/she must be informed of the following:

- who the data controller is (identity and contact details)
- who the data protection officer is (if relevant)
- why their personal data is being processed (for what purpose)
- the legal basis is for processing (consent, contract, etc.)
- what the legitimate interests are, in cases where the legal justification for the processing is balancing of interests
- who the information will be shared with (recipients), including processors

- whether the information will be transferred to a third country or international organisation

When necessary **to ensure fair and transparent processing**, the data subject must be informed of the following:

- how long the personal data will be stored
- data subject's rights to access, rectify and erase personal data. That it is possible to object to and put restrictions to the processing of personal data and whether there is a right to data portability.
- hat consent can be withdrawn at any time
- whether the processing of personal data is being performed as a result of contractual requirements, or is necessary in order to enter into a contract
- whether the use of the software entails automated decision-making or profiling, in which case they should also be provided with information about the algorithms and the significance/consequences of the processing
- whether the personal data is intended to be used for purposes other than those for which it was collected, and if so, what rights and regulations apply to this processing.

When personal data is collected from <u>persons other than</u> the data subject, **information** must be provided concerning:

- which categories of personal data are being processed
- the source(s) of the personal data and whether it came from publicly accessible sources

The software must make it easy for the **data subject to exercise their rights**, such as

- the right to access their personal data, information about the processing, and other rights
- the right to rectify their personal data as quickly as possible
- the right to delete their personal data as quickly as possible, if the conditions for deletion apply ("the right to be forgotten")
- the right to restriction of processing of their personal data, if the conditions for restriction apply
- the right to data portability for their personal data, if the processing is based on consent or agreement and is carried out by automated means
- the right to object against the processing of their personal data, if the preconditions for exercising the right to object are present
- rights relating to automated individual decision-making, including profiling that may have legal consequences, or similarly significant effect for the person concerned

- If the user has requested that personal data be rectified, deleted, or limited, the data controller must inform each recipient to whom the personal data have been disclosed.
- The software must pseudonymise personal data when there is no longer any need to have identifying personal data and anonymise or delete personal data when the purpose of processing is fulfilled.

- The software must contain safeguards preventing the linking of personal data about the data subject to other personal data in other systems, or to personal data collected for other purposes.

Requirements to fulfil the organisation's obligations
When using processors:

- The controller must only use processors who provide adequate guarantees that they will implement measures ensuring compliance with the data protection regulation and ensure the protection of the rights of the data subject.
- The controller must ensure that any suppliers and subcontractors fulfil all requirements by entering into processing contracts.

To ensure security of processing of personal data, it is necessary to

- ensure **confidentiality (C)**. Personal data must be secured against unauthorised disclosure or access.
- ensure **integrity (I)**. Personal data must be secured against accidental and unlawful destruction, loss, or alteration.
- ensure **accessibility (A)**. Personal data must be available to authorised personnel who require it for their work.

Additionally, the data protection regulation requires ensuring resilience (R), and we also recommend ensuring traceability (T):

- Resilience means that software that is processing personal data must be able to resist e.g. vulnerabilities, attacks, and accidents.
- Traceability is documentation of changes made within the software and to personal data. The purpose of traceability is to manage security breaches.

The OWASP Application Security Verification Standards (ASVS) (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project), like several other security standards, contain several security requirements for use in software development. We will not repeat them here, but advise everyone to evaluate the level of security required for software and software development. We also recommend applying the requirements of a comparable level to the OWASP ASVS standards.

Norway has several regulations setting security requirements within different sectors. Each individual business must ensure that it knows which rules it is subject to when developing software.

Listed below are a number of security requirements that can be implemented, and examples of which security principle it refers to (C, I, A, R, T).

- Access control:
    - The software has access control (authorisation, authentication, and traceability):
        - Users must be identified (T)
        - Which roles should have which rights (principle of least privilege) (A)
        - It is possible to control traceability when auditing logs (T)

    - Users are granted access only to information necessary for the performance of individual tasks (principle of least privilege). (C, T)
    - Administrator privileges are given to a small number of individuals based on principle of least privilege. (C, I, A, R, T)
    - The data subjects have access to their own personal data. (I, A)
    - Passwords are securely handled, and the software requires strong passwords. (C, I, A)
    - The software supports and requires strong authentication (such as two-factor authentication) where necessary (e.g., users may be encouraged to use it, while it is required of administrators and users with access to personal data requiring protection or personal data on multiple subjects). (C, I, T)
    - The software must monitor if and when anyone attempts to gain unauthorised access. (C, I, R, T)
    - The software must restrict access by third parties, and limit what a third party may access (e.g., restrict access to specified IP addresses or provide temporary and limited access). (C, I, R)
- The software must ensure that there is appropriate and sufficient information security during the storage and communication of data. Encryption can help to achieve this. When using encryption, widespread and recognised algorithms and methods must be used at all times, with a sufficient key length. Minimum requirements must be set for administration, specifying how often security algorithms must be reviewed and updated
    - at endpoints (PC, laptop, telephone, tablet) (C, R)
    - upon remote access (C, R)
    - upon transfer and storage via cloud services (C, R)
    - for backup and security copies, and units containing backup data (C, A, R)
- The software must protect the integrity of data and be able to detect changes in files, servers, and networks, by (I)
    - comparing hash values and checksums
    - limiting write access
    - regular integrity checks
    - setting reference values (min/max)
- The software must ensure that personal data is available when necessary through (A)
    - Redundancy
    - contingency plans
    - incident management
    - the software must be able to restore availability and access to personal data in a timely manner in the event of a physical or technical incident
- The software must be resilient. It must (R)
    - be secured against known security holes and vulnerabilities
    - be correctly configured
    - ensure segmentation of stored data, systems, processors, and networks
    - ensure that third party software and patches are kept up-to-date
    - be capable of receiving notifications from users and others about vulnerabilities in the software, and of ensuring that they are managed and taken seriously
    - ensure the secure destruction of media that process personal data
- The software must allow changes to be traced and enable management of security breaches by (T)

- documenting software and procedures
- logging configuration changes, processes, activities, and incidents
- access control to logs based on the principle of least privilege and only when access is specifically required
- deleting or anonymising logs after a given deadline
- not storing logs for longer than necessary

Acceptable level for risk for data protection and information security

- Establish tolerance levels for data protection and for information security. The purpose of setting tolerance levels is to define acceptable levels of risk for security and data protection in the software. These must be based on established and accepted supporting tables and tolerance limits.
- Define individual acceptable levels for risk for data protection and information security. Methodology can be reused.
- Auxiliary tables can categorise criticality levels e.g., Critical, High, Moderate, and Low. Enter variables for each category, and define the acceptable level of risk.
- Examples of categories that must have **acceptable levels for risk for data protection**:
  - The data subject must have control of their personal data.
  - The data subject must not loose his/her rights or freedoms.
  - The data subject must not be profiled or discriminated.
  - The data subject must not be subject to identity theft or fraud.
  - The data subject must not suffer financial loss.
  - The data subject must not suffer loss of reputation.
  - In cases of pseudonymisation, it must not be possible to trace back to the original identity without authorisation.
  - Confidentiality breaches of protected data must not occur.
- Examples of categories that must have **acceptable level for risk for security**:
  - There must be no accidental or unlawful destruction, loss, or alteration of personal data.
  - There must be no unauthorised disclosure of, or access to, personal data.
  - Personal data must be secured with regard to confidentiality, integrity, accessibility, and resilience of the software.
  - Personal data must be pseudonymised as quickly as possible, and encrypted.
  - It must be possible to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.
  - There must be a process for regularly testing, assessing and evaluating the effectiveness of measures for ensuring the security of processing.

EXAMPLE:
The company management has set the acceptable level for risk for the category "Damage to life and health" at 'Low' criticality. The red text (see table below) is beyond the company's acceptable level for risk. If information is compromised, there is a lack of information integrity, or a lack of access to information leading to 'Medium', 'High', or 'Critical' criticality, this will be unacceptable for the company's management, and measures must be implemented. Examples of situations in which information lacks

sufficient integrity resulting in 'High' criticality might include the provision of incorrect information about the brakes on a car, or about a person's blood type.

Criticality level	**Category – example:** Damage to data protection rights
Critical	Death or injury resulting in permanent disability
High	Damadge to reputation or social exclusion
Medium	Personal exposure resulting in sick leave
Low	No exposure

Microsoft SDL (https://www.microsoft.com/en-us/sdl/) and ISO 27034-x (https://www.iso.org/standard/44378.html) also provide examples on how to find acceptable level of risk.

Data protection impact assessment and security risk assessment

- The purpose of a data protection impact assessment is to assess the impact an envisaged software or processing operation may have on the protection of personal data. It is to ensure that the software does not infringe on the data subject's fundamental rights. The processing should, for example, be lawful, fair, and predictable. In certain types of processing of personal data it is required to carry out a data protection impact assessment:
  - In the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person,
  - when processing sensitive personal data on a large scale, or
  - a systematic monitoring of a publicly accessible area on a large scale.

  If you are in doubt about your obligation, we recommend you to carry out a data protection impact assessment.

- The assessment shall contain at least:
  - A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller,
  - an assessment of the necessity and proportionality of the processing in relation to the purposes,
  - an assessment of the risks to the rights and freedoms of the data subjects, and
  - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the data protection regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
- In cases where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk, the data

protection regulation requires that you contact the Data Protection Authority for a prior consultation.

- Carry out a technical risk assessment of the software's information security:
    - Such an assessment should reveal vulnerabilities and deficiencies in the security of the software, thus contributing to the provision of adequate security requirements.
    - Be sure to test, assess and evaluate the effectiveness of the security measures.
    - Please examine existing standards and examples of how to implement risk analysis, such as ISO27005 (https://www.iso.org/standard/56742.html), the Data Protection Authority guidelines on risk assessment (https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/risikovurdering/), and the guidelines for internal control and information security issued by the Agency for Public Management and eGovernment (Difi) (http://internkontroll.infosikkerhet.difi.no/).