Policy for the processing of personal data

Revised 07.08.2025

Gjensidige

Classified: General Business

Content

Policy for the processing of personal data		**3**
1.	Purpose	3
2.	Scope	3
3.	Definitions	3
4.	Roles and responsibility	3
5.	Requirements and methods	4
6.	Reporting	7
7.	Control	7

Policy for the processing of personal data

1. Purpose

The purpose of this policy is to establish detailed requirements for the processing of personal data. This policy intends to help ensure compliance with applicable data protection regulation, as well as customer's and employees' confidence that personal data is processed in accordance with applicable law.

2. Scope

This policy applies to the processing of personal data in Gjensidige Forsikring ASA and its subsidiaries (hereinafter called Gjensidige).

3. Definitions

- "Personal data" means any information relating to an identified or identifiable living natural person.
- "Special categories of personal data" (sensitive personal data) means:
  - information relating to racial or ethnic origin,
  - political opinions, philosophical or religious beliefs
  - trade union membership
  - processing of genetic information and biometric information for the purpose of identifying a natural person,
  - health information and,
  - information about a natural person's sex life or sexual orientation.
- The terms and conditions for processing data concerning criminal convictions and offences are the same as for the processing of special categories of personal data.
- "The data subject" is the one the personal data is related to.
- "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4. Roles and responsibility

Executive Vice Presidents (EVPs)/branch manager in Sweden

- Shall ensure that routines are established to meet current data protection regulations.
- Shall ensure that risk assessments and data protection impact assessments (DPIA) are carried out when this is required.
- Shall ensure that an overview is kept of which processing of personal data is carried out within their own area of responsibility.
- Shall ensure that the data subject's right to information is complied with.

Executive Vice President People & Communication

- Shall be responsible for ensuring that the processing of personal data about employees in shared processes, systems, and tools (e.g., in collaboration tools) is carried out in accordance with data protection regulations.

Data Protection Officer

- Shall provide advice in connection with Data Protection Impact Assessments (DPIA), be responsible for the DPIA procedure, assist in the assessments and control how the assessments are carried out.
- Additional tasks are described in Function description for second line functions.

Managers

- Shall be responsible for ensuring compliance with the data protection regulations within their area of responsibility, that employees have the necessary competence, working conditions and knowledge of applicable data protection regulations, and how to report data privacy breaches.

Group Procurement

- Shall ensure that data processor agreements are established in procurement processes with service providers who process personal data on behalf of Gjensidige.
- Shall establish routines for control of data processors' compliance with the data processor agreement.
- Is responsible for Gjensidige's template for the data processing agreement, responsible for registering the data processing agreement in the procurement system and for assessing whether provisions in the template can be deviated from after doing a specific assessment
- Shall coordinate the work related to conducting and documenting risk and security assessments related to procurements and outsourcing which includes processing personal data.

Group Security

- Shall assess the data processors' security level based on the data processor's response to the security document as part of the data processing agreement.
- Shall control data processors' compliance with security requirements according to a risk-based approach.
- Shall ensure that controls are documented and present this at the request of subsidiaries and branches.

IT-security

- Shall carry out IT security assessments, which includes assessment of privacy risks to ensure continued confidentiality, integrity, availability and robustness in systems and services where personal data is processed, including in procurement, outsourcing and development.
- Shall recommend actions to reduce risk.

Employees

- Shall within their area of responsibility contribute to compliance with applicable personal data regulation, complete mandatory training and register any data privacy breaches according to the applicable procedure.

5. Requirements and methods

5.1 Legal basis for processing personal data

Personal data shall only be processed if there is a legal basis for such processing. The most common legal basis used in Gjensidige is that the processing is necessary to fulfil an agreement with a customer or an employment agreement with an employee. Other relevant legal basis for processing are that the processing is necessary for the company to safeguard its interests (a 'legitimate interest'), that the processing is necessary for meeting legal obligations or to fulfil statutory requirements, or that Gjensidige has obtained the data subject's consent for the processing.

In order to process special categories (sensitive) of personal data, an additional special legal basis is required. The most relevant basis are consent, that the processing is necessary to establish, assert or defend a legal claim, that the processing is necessary to safeguard the data subject's vital interests, or that the processing is necessary to be able to safeguard important public interests.

If processing of sensitive personal data is necessary to enter into the agreement with the data subject, for example health data when purchasing personal insurance, consent must be obtained from the data subject.

To meet requirements for documentation, consent must be obtained in writing. If this cannot be done, oral consent must be registered and confirmed in writing to the data subject.

When processing personal identification numbers (cpr-number) in the Danish branch, processing is permissible only when authorized by law or with consent. Disclosure of personal identification numbers in the Danish branch may take place if it is part of normal operations, and such disclosure is of utmost importance to ensure a clear identification of the data subject or is required by a public authority.

5.2 Processing of personal data

In the event of new or changed processing of personal data, Risk-, Compliance-, and Security coordinator must be contacted for documentation of the processing activity in the relevant system support, this shall ensure compliance with essential requirements that follow from the data protection regulations. Group Compliance shall establish a

routine for how processing activities are to be documented.
Sensitive personal data, personal identification numbers and information about criminal offenses shall be handled with particular care and reassurance and be specified in routines.

5.3 Quality assurance, registration, and data minimisation
Whoever processes personal data must ensure that these are:

- lawfully collected,
- relevant to the business and limited to what is necessary based on one or more defined purposes,
- correct and up to date,
- limited to what is strictly necessary to achieve the purpose.

Personal data that does not comply with these requirements shall not be processed. In cases of doubt, the manager must be consulted.

All personal data must be registered so that:

- assessments, characteristics etc. of a subjective nature are not recorded. The data subject must as a main rule be able to receive registered information in full,
- information subject to the right of access is readily presentable,
- information that is not subject to the right of access can easily be excluded.

In the event where information is corrected, this must be communicated to relevant recipients of the information.

Information from social media and tips cannot automatically be considered reliable information, and any use must be assessed and documented. Such information shall only be collected if it meets the requirements mentioned above. If the source is anonymous, the assessment must be done with diligence. The data subject cannot be evaluated solely based on anonymous tips, and the source`s wish for anonymity cannot be guaranteed.

5.4 Purpose limitation and reuse
The reuse of personal data for purposes other than those for which it was originally collected is permitted if the data subject consents to the processing or the processing is necessary to fulfil a legal obligation under national law. In other cases, personal data can only be used for other purposes if the new purpose is not incompatible with the original one. This can be determined by taking into consideration:

- Any connection between the original and new purpose
- In which context the information has been collected
- The reasonable expectations of customers and other data subjects with regard to the reuse of the information
- The nature of the personal information
- The consequences of intended reuse for customers and other data subjects
- Necessary safeguards, which may include encryption or pseudonymization.

The above assessment must be documented, and Group Compliance shall provide a template that can be used for this purpose.

5.5 Use of personal data for testing purposes
As a main rule, personal data must not be used in tests. Testing must, as far as possible, rely on fictitious or anonymized data. When this is not possible, pseudonymised personal data can be used. Personal data can only be used in a test if it can be documented that it is necessary to achieve the purpose of the test.

EVP Technology and Insight must implement routines for the use of personal data for test purposes, including how necessity assessments are to be carried out.

5.6 Privacy by design
Suitable technical and organizational measures must be developed to effectively implement the principles for the protection of personal data. Data privacy must be taken into account throughout all development phases of a service, product, system or solution, and the most privacy enhancing standard settings shall be implemented.

EVP Technology and Insight must implement routines that ensure that requirements for privacy by design and by default are being implemented.

5.7 Storage
Personal data shall as a main rule be registered and stored in professional systems, ensuring it can be easily found by searching for the data subject. If this is not possible, personal data must be stored in dedicated folders in the

file area (R:). Personal data can be stored in the e-mail system if it is being processed.

Storage of personal data on Teams or Sharepoint must follow Gjensidiges classification rules. Information classified as "Confidential Privacy" shall not be stored on Teams or Sharepoint, but in a dedicated folder in the file area (R:).

Physical documents must be handled properly and according to routines.

5.8 Disclosure
For the disclosure of personal data to other companies in the group, consent is required, unless otherwise stated in national legislation.

Various public authorities may require the disclosure of personal data.

Insurance companies can exchange personal data when there is concrete suspicion of fraud, unless otherwise stated in national legislation. In this case, the Investigation unit must be contacted before personal data is disclosed to another company.

5.9 Deletion
Personal data that is no longer necessary to fulfil the purpose of the processing must be deleted, unless there are regulatory requirements for further storage. Deletion means that the personal data is removed in a way that it cannot be restored. Automatic deletion routines must be established in systems that store personal data. For all other storage, manual procedures for deletion must be established.

For customers whose customer relationship has ended due to fraud, and with registration of an unwanted future customer relationship, customer information must be kept during the period the customer is unwanted, unless otherwise follows from national legislation. Deletion beyond the unwanted period then follows the regulations for limitation periods.

5.10 Anonymisation and pseudonymisation
Information used for analysis and statistics must be anonymised. Anonymisation means that the information can no longer be linked to individuals. If the purpose cannot be achieved by anonymisation, the information must be pseudonymised. Pseudonymisation means that the information can no longer be linked to individuals without additional information that is stored separately from the information.

5.11 Obligation to provide information when collecting and disclosing personal data
When collecting personal data, the data subject must be informed about the collection and processing of personal data. The information shall as a main rule be provided through the privacy policy on Gjensidige's website or in standard information included in the application, claims report or insurance terms. As a starting point, the information must be provided at the time the personal data is collected. EVP Private shall ensure that a privacy policy and cookie declaration is updated and made available for Gjensidige Forsikring ASA Norway and the Danish branch.

Information that personal data has been collected from someone other than the data subject must be made available to the data subject no later than one month after the information has been collected. If the personal data is to be disclosed to another recipient, the data subject must be informed at the latest when the personal data is first disclosed.

EVP People & Communication must ensure that the obligation to provide information relating to employees is met in standard information provided in the recruitment process, and as an attachment to the employment agreement. A privacy statement must be made available that describes Gjensidige's processing of personal data about employees and their rights.

It may be omitted to provide information if the collection or disclosure of the information is stipulated by law, impossible or disproportionately difficult to provide, or if the data subject already knows the information. Furthermore, information may be omitted if it has been prepared exclusively for internal case preparation, has not been disclosed to others, and is necessary to ensure proper internal case management.

During an investigation, the obligation to provide information can be postponed until secrecy is no longer required for reasons of prevention, investigation, disclosure and prosecution of criminal offences. It must be assessed in the individual case whether notification may be of hinderance to solving the case. If the police have started an investigation, their needs must be clarified before Gjensidige notifies the data subject. The timing and content of the notification must follow internal rules.

If personal information is to be used for purposes other than those for which it was collected, the obligation to provide information needs to be fulfilled once more.

5. 12 The data subject's rights
The company must make sure the data subject is able to exercise their rights, including the right to information, access, correction, deletion, restriction, and the right to object to the processing.

EVP Private and Commercial and branch manager in the Swedish branch shall implement routines for how to handle requests from the data subject within their area of responsibility.

For Gjensidige Forsikring in Norway and Denmark EVP Private shall be responsible for the technical right of access solution as well as coordinate answers to right of access requests.

EVP People & Communication must implement routines for how employees can exercise their rights.

Anyone who suffers damage as a result of a violation of the General Data Protection Regulation (GDPR) may be entitled to receive compensation from Gjensidige for the harm caused. Group Compliance shall prepare a procedure for how compensation claims are to be handled.

5.13 Incidents
A data privacy breach (personal data breach) means a breach of security that leads to unintended or unlawful destruction, loss, amendment, unlawful dissemination of or access to personal data that are transferred, stored or in other ways processed. Reference is made to the governing document for incident registration for more detailed procedures for dealing with personal data breaches.

5. 14 Data processor agreement
If others process data on behalf of the company, a separate data processor agreement (in addition to the service outsourcing agreement) must be entered into advance, which as far as possible is in accordance with Gjensidige's template for data processor agreement. The contract owner is responsible for entering into a data processor agreement.

5. 15 Risk assessment
5.15.1 Assessment of personal data security
As part of the risk assessment related to security, an assessment of personal data security must be carried out. IT security must ensure that this is done in collaboration with the manager for the relevant area. The risk assessment must be based on the risk to the data subject and identify potential events that could lead to accidental or unauthorized (illegal) access, change, deletion, loss or disclosure of personal data.

5.15.2 Data protection impact assessment (DPIA)
If it is likely that a type of processing will entail a high risk for the data subject's privacy, rights and freedoms, the immediate responsible manager must ensure that a DPIA is carried out. Group Compliance shall implement a routine for the process of DPIA.

5.15.3 Transfer outside the EEA
The manager is responsible for carrying out a risk assessment (TIA - transfer impact assessment) when transferring personal data outside the EEA. The assessment must be done in collaboration with Group Procurement, who involves the data protection officer if necessary.

6. Reporting
EVPs and branch manager in Sweden must report privacy risks in their own area as part of the annual risk assessment process to the CEO.

The data protection officer must report quarterly to the board and management on compliance with the data protection rules through the Risk and capital report.

EVPs and branch manager in Sweden are obliged to inform relevant second- and third line functions about conditions that are relevant to the performance of their tasks. Deviations from the provisions in this document must be reported in accordance with the governing document for registration and reporting of operational incidents. Second- and third line functions have the right to obtain the information and access what they request in order to carry out their work.

7. Control
EVPs and branch manager in Sweden must establish proper controls to ensure compliance with this policy, which contains at least:

- Updated overview of personal data processed
- Routines for manual deletion
- Updating the privacy policy in case of new processing of personal data
- Access control