Protection of privacy and data security

This is a summary of our protection of privacy and data protection measures, as they are described on our Norwegian website (https://www.gjensidige.no/privat/bank/personvern-og-sikkerhet).

Processing of personal data

Gjensidige has obtained a licence from the Norwegian Data Protection Authority and has rules for how to process personal data.
Personal data are pieces of information that can be linked directly to a person, for example a customer's personal ID number, address, phone number etc. We need this type of information to be able to provide banking, insurance, savings and pension services to our customers.

For some of our services, we need to collect and process sensitive personal data, for example medical information. Particularly stringent requirements apply to access to and processing of sensitive personal data.

Customers are informed when we collect information about them, unless:

- the collection is regulated by law
- notification is impossible or disproportionally difficult
- there is no doubt that customers already know the information to be contained in the notification

We communicate with our customers by email. When we send sensitive personal data or personal ID numbers by email, we encrypt the information to ensure that unauthorised persons cannot gain access to it.

We recommend that our customers never send sensitive information by email, to us or anyone else.

Consent

Gjensidige's processing of personal data is based on customers' consent. The consent must be explicitly stated, voluntary and informed, so that the purpose of the processing is clear.
The collection of sensitive data requires separate consent. Customers can change their consent settings by logging on to our customer portal.

Disclosure of personal data

Internally in the Group

All Gjensidige employees have a duty of confidentiality concerning customer data.
Gjensidige has a central customer register, but only neutral personal data can be disclosed to other companies in the Group for the purpose of administration and customer care, including marketing, without the customer's specific consent.

To the insurance companies' joint registers

All companies that sell life insurance or other accident and health insurance share some personal data in a joint register that is administered by Finance Norway, an industry organisation for the financial industry in Norway. The register does not contain sensitive personal data.

The purpose of the register is, among other things, to:

- reduce the probability of misunderstandings in connection with the purchase of insurance
- reduce the probability of incomplete or incorrect information or insurance fraud

In order to prevent and limit insurance fraud in connection with claims reports and settlements, the insurance companies have a joint claims register. The register is administered by Finance Norway.

Customers shall be informed that data will be stored in these registers.

To Økokrim (the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime) when money laundering or financing of terrorism is suspected

Money laundering is the process of transforming the proceeds of crime into legitimate assets that can be used openly in the legal economy.

Gjensidige has a duty to prevent and combat money laundering and to prevent people from using the company for money laundering of the proceeds of crime.

The same applies to financing of terrorism.

Disclosure of personal data without customers' consent

In some cases, we are required by law to disclose data to others, for example public authorities or a spouse. In such cases, information may be disclosed without customers' consent.

Storage of personal data

The information we have about customers is stored in our customer register and in various case processing systems, among other places. The information is stored for as long as it is necessary to fulfil the purpose of the processing. In practice, this means as long as the customer relationship exists.

If a customer terminates a product or service with us, we will, due to the possibility of future insurance claims that can be traced back to the agreement, store the information until the limitation period for the products in question has expired.

Customers' rights

Access

Customers are entitled to information about the personal data we have registered, and to know where the data were retrieved from and how we process them.

Gjensidige's duty to provide information

Customers shall be notified when we collect personal data about them. Our duty to provide information applies even if customers have consented to the collection.

Correction and deletion

Customers can demand that information about them be corrected if it is incomplete or unnecessary.

Gjensidige deletes registered information when we no longer need it to fulfil the purpose for which we collected it, unless we are obliged by law to store it longer.

Reservation

Customers can activate the option of not receiving direct marketing material by logging into the customer portal and changing their consent settings.

Gjensidige's data controller

The data controller is the person who decides the purpose of the processing of personal data and what tools are to be used. The data controller is responsible for ensuring that measures are implemented to meet data protection regulations, including that requirements are drawn up for internal control and information security.

The companies have established the role of day-to-day data controller, who is tasked with keeping an overview of the processes, business areas and systems that process personal data and following up internal control and the risk situation on a continuous basis.

The data controllers in the companies:

- Gjensidige Forsikring ASA – The role of data controller is delegated from the CEO to the EVP of Product and Price
- Gjensidige Bank ASA – CEO
- Gjensidige Pensjonsforsikring ASA – CEO

Permission in Gjensidige's apps

Gjensidige has a bank app and an insurance app. Both request the customer's permission to enable the apps to deliver the services and experiences as intended. This permission will not be used for other purposes. We inform the customers about the type of permission the apps require and why.