Contents

Safeguarding your privacy

At SpareBank 1, we take your privacy seriously and always strive to ensure that your personal data is secure with us. You can read more about how we process your personal data in this privacy policy.

The privacy policy has been updated 12.06.2025

Who is responsible for your personal data?

This privacy policy is for customers, potential customers and other users of SpareBank 1's services and websites. SpareBank 1 is made up of a number of banks and companies. Where "SpareBank 1" or "we" is written in this policy, we mean banks and companies in SpareBank 1.

Controller

It is the bank and/or companies you have a customer relationship with in SpareBank 1 that are responsible for processing your personal data. If you need to contact us in relation to privacy, please email the data protection officer at the bank or institution.

Download our privacy policy

You can download our privacy policy as a PDF here.

Safeguarding your privacy. Download our privacy policy (PDF in English).

Cooperation within SpareBank 1

SpareBank 1 consists of a number of companies that in some circumstances cooperate on how your personal data is processed. This applies, for example, when you buy insurance or sign a credit agreement. For answers to any questions you may have, please contact the bank or company of which you are a customer.

Information about you will never be shared between the banks.

How we use personal data

Your information is primarily used for the purposes of customer management and to fulfil our obligations to you. We also use personal data to provide you with information, offers and to fulfil our legal obligations.

Providing agreed services

Accounts and payments

When you are a customer of ours, we collect and use your personal data to perform transactions and services for you, as well as to fulfil our legal obligations. We use personal data when, for example, you open a new account or sign a payment service agreement with us. This enables us to send you invoices, carry out payments and provide other agreed services.
The online and mobile banks provide overviews of your accounts and transactions. You can also identify your subscriptions or other recurrent expenses, which we can help you cancel.

Basis for processing: Agreement, legal obligation

Card payments

We use your personal data to provide you with payment solutions such that you can pay in physical stores and online. This includes payments from your bank accounts using your bank cards, mobile phone or other technical devices.

We also use your information to help prevent you from being scammed.

Basis for processing: Agreement, legal obligation, legitimate interest

Loans and other credit

We use your personal data when you apply for a loan from us. This applies whether you have applied for a loan secured by a mortgage in real estate, for example, a home, holiday home or line of credit, a credit card or a consumer loan. To determine whether we can approve the loan, we need to check your credit rating in addition to processing the loan application itself.

We also process any co-borrower's and/or guarantor's personal data. Once the loan agreement has been signed, we use your personal data to monitor your customer relationship and register ongoing loan repayments.

We use fully or partially automated credit processes. Automation means that decisions are made without manual human processing. If decisions that will significantly affect you will be made by fully automated processes, we will inform you of this in advance. In these circumstances, you may request manual case processing.

Basis for processing: Agreement, legal obligation

Risk classification of customers and credit portfolios

We use your personal data to assess the risk associated with sales of products and services. This means that you, the customer, can be confident that your assets will be well taken care of.

We are legally required to process credit information, application information and other information about you in order to calculate capital requirements for credit risk. Such processing is performed when you establish a customer relationship and when assessing which services and products are suitable for you.

The calculations are performed using our own models, work and decision-making processes, and internal guidelines. This applies to the classification and quantification of credit risk and other risks. In other words, the risk associated with credit and other financial factors is assessed.

Basis for processing: Legal obligation

Savings and investments

We use your personal data to open and service your savings accounts, for example, share savings accounts (ASK), as well as to provide investment services to you. To provide investment services, we need to collect information about you that enables us to assess your suitability and appropriateness with respect to the intended investment service or investment product, such as portfolio management or trading in stocks, bonds and securities funds.

We are legally required to ensure all investment services are documented. This means that we record all phone calls and retain all electronic communications when we provide investment services to you.

A number of our savings products are provided by our partners and, therefore, agreements will have to be signed with both the bank and our relevant partner.

Basis for processing: Agreement, legal obligation

Insurance

We use your personal data to provide you with insurance, for example, non-life insurance and pensions. The personal data we process depends on the insurance agreements you have with us. For example, we process health data if the insurance is a personal insurance policy and data about your vehicle if the insurance is a car insurance policy.

Our insurance products are provided by our partners and, therefore, agreements will have to be signed with both the bank and our relevant partners.

Customer service

We want to be available to our customers both digitally and physically, in order to provide the best possible customer service and advice. Our digital bank is our preferred channel for communicating with you safely and securely. We are also available via email, chat, letter, phone, meetings and other channels, such as social media.

Chat

Our chatbot is designed to streamline customer service and respond to simpler enquiries from you. That is why all chat conversations start with our chatbot. In some cases, we use artificial intelligence (AI) to enable the chatbot to understand questions and provide you with appropriate answers. Such answers are provided with the proviso that responses may contain errors.

Should you wish to speak to an adviser during the chat, the adviser will have access to the chatbot conversation so that they can familiarise themselves with your enquiry. You can download the chat transcript once it has ended.

When you start a chat conversation while not logged in to our websites, we only process your IP address. The chat conversation may be used for the purposes of statistics and customer service evaluation. Such conversations are only linked to your customer relationship when you have logged in to the digital bank so that we can provide the best possible customer service.

Your chat conversations may be used for the purposes of analysis and improving the chatbot. However, we will always ensure that any personal data is anonymised first such that your conversations can no longer be linked to you when they are analysed.

Basis for processing: Agreement, legitimate interest

Phone and voice

In some cases, you may come into contact with our voicebot in order to receive more efficient customer service by phone. Based on what you need help with, our voicebot will connect you to an appropriate adviser who can help you further with your enquiry.

Customer enquiries processed by our voicebot are subject to spot checks to test whether it is functioning as intended and to improve responses. To these ends, voicebot conversations are recorded for review as part of the work on improvements. Audio files containing personal data will be excluded from such improvement work.

Otherwise, we retain summaries of your conversations with advisers. Such summaries are stored against your customer relationship in order to follow up and document your enquiry. Summaries can be created with support from AI.

Basis for processing: Agreement, legitimate interest

Marketing

We want to be relevant to you and, therefore, process your personal data for the purposes of providing you with personalised advice and offers. In order to market our products and services, we process your name, contact details, date of birth and what services or products you have with us or our partners.

If you have consented to it, we may also process, for example, your transactions, which includes compiling and analysing other information, such that we can personalise our communications, advice and offers to ensure that they are even more relevant to you.

We will respect your marketing opt-outs.

Basis for processing: Consent, legitimate interest.

Customer and market research

We use your personal data in connection with market and customer satisfaction surveys. For example, we may ask about your experience after you have been in contact with us. Feedback from our customers helps us improve ourselves and our products and services. We can also measure the effectiveness of improvements and examine the link between customer satisfaction and customer behaviour over time. Responding to such surveys is voluntary.

Basis for processing: Legitimate interest

Preventing and detecting criminal offences

We use your personal data for the purposes of preventing, investigating and reporting economic crimes and other criminal offences against you, other customers or us. This is required by law and our obligations.

We also use personal data to perform sanctions monitoring in line with the specific regulations concerning this with the aim of identifying customers and transactions subject to international sanctions and restrictive measures.

Basis for processing: Legal obligation, legitimate interest

Security

We constantly strive to ensure that your personal data is secure. The measures we employ include access management, logs, encryption, firewalls, access controls, and video surveillance, as well as other measures that safeguard your security and our security. In some cases, these measures may involve us processing your personal data, for example, by video surveillance. We have governing documents and procedures for information security, nonconformance management and employee training.

Logging in

One important security measure is to identify you as a customer and secure confirmation of your identity (authentication). We use BankID to be certain of who is logging in. How your personal data is processed when you use BankID is described in the *terms and conditions for BankID (PDF) and in BankID's privacy policy*.

Basis for processing: Consent, agreement, legal obligation, legitimate interest

Video surveillance

We have installed video surveillance in our premises and for our ATMs. Recordings are retained for up to 90 days. They may be retained for longer if the recordings will be used for other purposes by us or the police.

Basis for processing: Legal obligation. Legitimate interest

Logs

Your activities in the online and mobile banks are logged in order to track what changes have been made and by whom. Corresponding logging takes place in our internal systems where we process your personal data. The logs can be used, for example, in the event of a system failure or breach of security. We have a legitimate interest in logging such traffic in order to identify or prevent undesirable activities in or against the bank. Such logging takes place to the extent that is strictly required and proportionate to ensure good information security.

Basis for processing: Agreement, legal obligation, legitimate interest

Governance

We use your personal data for the purposes of ensuring good corporate governance. We analyse personal data to gain insights into what our customers need and expect. These insights make it easier for us to identify potential demand for new products and services, and to improve the functionality of existing products and services. Such insights also better enable us to structure the organisation properly, which includes ensuring that we have the right capacity and expertise in the right place.

Basis for processing: Legitimate interest

Service development and testing

We constantly strive to improve and enhance our systems, services and products. As a general rule, we must use fictional or anonymised data when developing and testing our solutions, although sometimes we have to use personal data to ensure functionality and security.

Basis for processing: The basis for processing is compatibility. This purpose is closely associated with our original purpose of providing agreed services to you.

Statistics

We also use personal data to produce statistics, both for our own purposes and to share statistics with public and other private organisations. The statistics consist of aggregated data that cannot be linked to you. The personal data we will use depends on the purpose of each statistics task.

Examples of statistics may include what time of day most people go grocery shopping, how many customers live in a detached house or what the average person in a municipality spends on electricity, phone subscriptions or food consumption. Statistics may also be used in connection with sustainability reporting or product development.

Basis for processing: Legitimate interest

Documentation to protect our interests

We use your personal data so we can establish, enforce or defend legal claims related to you. We retain documentation and history relating to your customer relationship for as long as you can make a claim against us. How long we retain such documentation is determined by the limitation period.

Basis for processing: Legitimate interest

Audits and inspections

We use your personal data for the purposes of checking and ensuring that we are organised and conducting our business responsibly. The checks are carried out on an ongoing basis, for example, through spot checks, topic checks and internal and external audits. Your personal data may be included in the checked data, for example, when we check the quality of the data we collect in connection with anti-money laundering work.

We monitor our activities and process personal data in connection with this. Such checks are carried out by the company's own employees, contracted auditors and the authorities.

Basis for processing: Legal obligation,

Profiling

We use your personal data for the purposes of profiling such that we can provide you with specific services and products that match your preferences, prevent and detect money laundering, fraud and other financial crimes, set prices assess probability of default, and assess the value of assets.

You have the right to object to profiling.

Basis for processing: Legitimate interest, consent

Your rights

Your rights when we process your personal data are described below.

Right of access

You have the right to request access to the personal data we process about you, and you have the right to receive a copy of this information. You also have the right to information about how we process your data. Information about this can mainly be found in this privacy policy.

Information about, for example, your products, agreements, contact information and transaction history are available in your online bank. If you cannot find the information you are looking for, please send us a request for access. We may ask you to clarify what information or processing activities you want to access. In those circumstances where your online bank is not available or you cannot read electronic documents for some other reason, we can send you the information on paper.

There are some exemptions to the right of access. These include when we have a legal duty of non-disclosure or we have to keep information confidential for the prevention, investigation, detection and prosecution of criminal acts. Another exemption exists regarding information that is solely contained in documents prepared for internal use and where exemption from the right of access is necessary to ensure proper processing.

You have a right of access to what personal data the company processes about you. However, you may not have a right of access to the names of employees who have viewed the personal data.

Right to rectification

It is important that the information we have about you is correct. SpareBank 1 checks its data against the Norwegian Population Register and other sources. At regular intervals, we also ask you in your online or mobile bank to confirm that the information we hold about you is correct. If you believe that the information we hold

about you is incorrect or incomplete, you have the right to request that the information be corrected or updated.

Right to erasure

You have the right to request that your personal data be deleted if:

- You withdraw your consent to the processing and we have no other basis for processing it.
- If you exercise your right to object to the use of your personal data and there are no compelling grounds for the processing.
- You say no to the use of your personal data for direct marketing purposes.

In many circumstances, we have to retain information about you, even though you want the information deleted. This may be true both while you are a customer of ours and for a period after the agreement with us has ended. In practice, this means that you may not always be able to require us to delete your data. This may be because we have a legal duty to retain it or because we must safeguard our legitimate interests. Similarly, we may need to retain your information to establish, exercise or defend a legal claim.

Right to restrict processing

You can require that SpareBank 1 restrict the processing of your personal data in certain situations, for example if:

- You believe that the personal data is incorrect or that the processing is not lawful.
- SpareBank 1 wants to delete the data, but you need the information due to a legal claim.

You have said no to the processing and we must assess whether we have good grounds for continuing the processing. We will still retain the relevant information, although all other processing of the personal data will be temporarily suspended. We may begin processing your personal data again in connection with legal requirements or to protect another person's rights.

How to retrieve your personal data

You can find and download the information you need directly in the online bank without having to retrieve all of the information at once (data portability).

Name and contact information
Your name, national identity number, email, phone number and address(es) can easily be found under settings in your online bank.
If you want to share your information with another provider, you are free to do so directly.

Account information and transactions
An overview of your accounts can be found in the account overview in your online bank.
For a detailed overview of your transactions, you can easily export a full list of transactions. The list is downloaded as a CSV file, which can be opened as a spreadsheet. Select an account, click on “Export”, and choose the time period for which you want to view transactions.

If you would like details pertaining to your insurance cover, you can fill out a simple form with your BankID, and Fremtind Forsikring will make them available to you within 30 days.

Right to object

You can ask us to stop processing your personal data if we are processing it based on our legitimate interests. This will apply unless we have important grounds that override your interests, or we need the information to establish, enforce, or defend a legal claim. You can also ask us to stop using your personal data for direct marketing, including profiling for this purpose.

If you wish to opt out of direct marketing, please contact customer services.

Exercising your rights

If you wish to exercise your rights, you can contact our data protection officer or customer service.

Email is considered an unsecure channel. We recommend that you do not send us confidential information via email. We will respond as quickly as possible and within no more than 30 days. If it is clear to us that the matter will take longer than 30 days to process, we will let you know.

If you have consented to marketing, you can change your mind at any time in your online or mobile bank.

Personal data collected

Personal data includes information and assessments that can be linked directly or indirectly to you as an individual. We process personal data about you based on what products and services you have with us.

Types of personal data collected

- Identification and personal information such as name, national identity number, citizenship, other identification numbers issued by the government and copies of proof of identity.
- Contact details such as phone number, address and email address.
- Financial information such as customer and product agreements, credit history, account numbers, balances, payment card numbers and transaction data.
- Information on income, assets, debt, place of work and employment, education, marital status, family relations and dependent responsibilities.
- Messages and summaries of conversations with the bank.
- Personal data that we are legally required to collect, for example, residence for tax purposes, foreign tax registration number, data in connection with anti-money laundering and terrorist financing efforts, and data for assessing your suitability and appropriateness with respect to investments.
- Health information in connection with purchases of personal insurance policies.

- Trade union membership when such membership affords you banking benefits.
- Photos and video recordings, for example, through video surveillance in our premises.
- Audio recordings, for example, when you speak to customer service and when we provide investment services.
- Online behaviour on our websites and in the online and mobile banks.

Where do we get your personal data?

From you

As a rule, the personal data we hold about you was provided directly by you as a customer, for example, when you opened an account, applied for a loan or contacted us via digital channels and chat.

From third parties

We collect information about you from others in order to provide services for you, to comply with legal requirements and to quality assure information you have provided to us. Examples of obtaining information from third parties, such as publicly available sources/registers or private business sources, could include:

- Identity information, family relationships, demographic information and information about collateral from the Norwegian Population Register, Eiendomsverdi AS, Norwegian Property Register or Register of Motor Vehicles.
- Collecting credit information and debt information about you from, for example, the debt registers and credit information agencies when you apply for a loan.
- Payment information from payers or recipients, shops, banks, payment service providers (such as Vipps and PayPal), billers (such as Tietoevry and Nets) and others.
- Information from public authorities such as the tax authorities, Brønnøysund Register Centre and the police. We also collect information from sanction lists published by Norwegian authorities and international organisations such as the UN, EU and Office of Foreign Assets Control (OFAC).

- Information about corporate customers' key persons and beneficial owners. The information is collected from the Brønnøysund Register Centre and commercial information services that provide information about matters that include rightful owners and politically exposed persons.
- If you consent to it, we can, in line with the payment services directive, exchange account and transaction information with other banks or financial companies. This means, for example, that you can see accounts from other banks in our mobile bank and vice versa, and that you make payments from them.
- Publicly available information, for example from social media or search engines.

From cookies

We collect information about how you use of our websites, platforms and digital apps such as traffic data, location data and other communications data. Read more about our use of cookies here.

Legal basis for using your personal data

We must have a legal basis for using your personal data. Four legal bases are particularly relevant for us.

Agreement with you

We use personal data based on an agreement we have signed with you. Any agreement we have signed, or will sign, with you must clearly describe the terms and conditions such that you can understand the personal data processing associated with the agreement.

Legal obligations

We also process your personal data to meet our legal obligations. For example, we are required to:

- Prevent and detect criminal acts such as money laundering, terrorist financing, scams, and fraud
- Monitor sanctions
- Keep accounting records
- Report to public authorities
- Classify risk related to risk management such as credit performance, credit quality, capital adequacy and insurance risk
- Rate credit worthiness
- Meet requirements and obligations related to payment services
- Meet other obligations related to service or product-specific legislation such as securities, funds, collateral security, insurance or home loan mortgages

Legitimate interest

We may use your personal data if this is required to safeguard a legitimate interest that outweighs considerations concerning your privacy. The legitimate interest must be legal, pre-defined, real and factually rooted in our business activities.
Examples of processing based on legitimate interest include:

- Analyses that enable us to improve our solutions and provide our customers with the best possible services, products and offers.
- Analyses, checks and reporting that enable us to develop our business and systems, as well as ensure good governance.
- Profiling, in order to, for example, personalise advice and offers or detect money laundering, scams and other financial crimes.
- Transaction classification of your expenses and income in order to provide you with a better overview and understanding of your personal finances.
- Automatic transfer to your SpareBank 1 bank when you log in to your mobile bank, so you do not have to disclose your bank affiliation every time you log in.
- Developing machine learning models in order to identify suspicious transactions in connection with statutory anti-money laundering efforts.
- Using machine learning and artificial intelligence to classify your transaction details, including in order to provide you with a better overview of where your money goes.
- Identifying your subscriptions or other regular expenses that we can help you terminate.

When we process personal data about you on the basis of our legitimate interests, you can object to the processing. Read more about the right to object under *Your rights*.

Consent

In some cases, we will ask for your consent to process personal data. The consent will state how we will use your personal data. You are free to withdraw your consent at any time. You can access an overview of your consents under settings in your online or mobile banks. You can also change your consents here.

Disclosure of personal information

We have a duty of non-disclosure regarding customer information. However, in some cases, we are legally required to disclose information about you to, for example, public authorities. We may also be permitted to share it with payment service providers, companies in SpareBank 1, or other parties. We always ensure compliance with the duty of non-disclosure no matter what.

Internally in SpareBank 1

The duty of non-disclosure applies between the banks and the companies in SpareBank 1, with the exception of the following information:

- Your name
- Contact information
- Your date of birth
- Information about the SpareBank 1 company in which you are a customer and the services and products you have entered into an agreement to receive.

Sharing such personal data will enable us to ensure correct and consistent information about our customers, as well as to personalise advice and offers. The exception only applies to banks, subsidiaries and product companies, and not between banks.

If you would like more relevant advice and offers, you can consent to us sharing more information about you. You will find the consent options in your online and mobile banks.

To public authorities

Your personal data will only be disclosed to public authorities when this is required by a statutory duty of disclosure or right of disclosure. We are legally required to disclose personal data to, for example, the Norwegian Tax Administration, the Norwegian Labour and Welfare Administration (NAV), the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim), the police, the courts, supervisory authorities, and public tribunals.

Norway has also signed reciprocal tax reporting agreements with a number of countries in order to combat tax evasion and international tax crime. The agreements are often referred to as CRS (Common Reporting Standard) and The Foreign Account Tax Compliance Act (FACTA). Under the agreement, Norwegian financial companies are required to identify and report persons, companies and other entities that reside or are domiciled abroad to the Norwegian tax authorities. You can get more information about CRS and FATCA from the Norwegian Tax Administration.

To other entities

If we are legally permitted to, personal data may be disclosed to other banks, insurance companies, financial companies, and partners. One example where this might happen could be if you want to see your account information in another bank, or if you want to see your insurance from Fremtind in your mobile bank. This will also apply in circumstances where the bank is obliged under, for example, the Norwegian Money Laundering Act to disclose information.

For payments to or from abroad we will provide pertinent personal data to the foreign bank. The laws of the recipient country determine the extent to which the information is disclosed to government agencies or regulatory bodies. This might be done to comply with the recipient country's tax laws, measures against money laundering or terrorist financing.

If you default on your credit agreements, the information may be disclosed to a debt collection company for the purpose of collecting the defaulted claim on behalf of the creditor. The claim may also be sold to a debt collection company which then takes over as creditor for the claim.

Use of data processors

We use third parties to deliver services to you as a customer. If these third parties process your personal data, they will be our data processors.

We sign data processing agreements with all providers that process personal data on our behalf. Such agreements regulate how a data processor can use personal data to which it gains access. We will only use data processors that guarantee compliance with the Norwegian Personal Data Act and GDPR.

Transfers out of the EU/EEA

We primarily prefer to only use data processors based in the EU/EEA. If SpareBank 1 uses providers outside the EU/EEA area, we will ensure that the following conditions are met to ensure that the privacy and rights of our customers are well safeguarded:

- There is an approved transfer basis for the delivery of personal data to a third country, such as the use of standard contracts (EU standard clauses) approved by the European Commission, the data processor has valid, binding corporate rules (BCR) or the European Commission has decided that there is an adequate level of protection in the relevant country.
- The level of protection for the processing of personal data in a third country has been assessed as corresponding to the level of protection in the EU/EEA, as a result of specified technical and/or organisational measures.

How long do we retain your personal information?

We retain your personal data for as long as necessary for the purposes for which they were collected and processed, unless statutes or regulations require us to store them longer.

For as long as necessary

As a rule, we retain your personal data for as long as necessary to fulfil an agreement you have entered into with us, or in compliance with the requirements for retention time in laws and regulations. After that, they are deleted or anonymised.

In cases where retention of your personal data is based solely on your consent, and you withdraw your consent, we will stop collecting data based on the consent and delete the data as soon as possible.

Examples of retention times

- Offer of product or service: up to 6 months after you received the offer
- Documentation collected and produced in order to prevent and detect money laundering and terrorist financing: 10 years after completion of the transaction or the end of the customer relationship
- Information we are required to keep under the Bookkeeping Act and bookkeeping regulations: up to 10 years
- Audio recordings of investment services: at least 5 years, and if deemed necessary up to 13 years
- Data collected for calculating capital requirements for credit risk: up to 50 years
- Documentation and history related to the performance of an agreement with you: up to 13 years after the end of customer relationship (this corresponds to the period during which you may, on a specific terms, make claims against us under your agreement, so-called period of limitation)
- Log backup: retained for as long as appropriate for the individual service

How we use cookies

It is important to us that you feel secure when you visit our website, and at the same time that we are doing our best to provide you with what you need.

What are cookies?

We use cookies in our digital channels: websites, online bank and mobile bank.

Cookies are small pieces of data that are stored on your computer or your mobile phone by the browser or app you are using. A cookie belongs to a specific website and therefore cannot be read by other websites.

If you use our website without identifying yourself, the cookie consent will only apply to the device (such as mobile or PC) you are using. When logging in to your online or mobile bank, you can choose to allow the answer from the device to apply to you as a customer as well.

You can choose which categories of cookies we can use.

Read more about our use of cookies here.

Cookies, pixels and scripts used by us

Technical cookies

For the websites to work, we must use technical cookies. These, therefore, cannot be turned off.

Functional cookies

We use functional cookies so that you do not have to go through the same choices every time you are on our websites. They store information about your use of the website and the settings you have selected.

Cookies that archive statistics

We use cookies that store statistics to make our websites better and simpler to use. This information helps us understand how the websites are used, which in turn enables us to improve.

Cookies for targeted marketing

For you to obtain content that is tailored to you, we use cookies that collect information about your usage pattern and your interests. This means that we can present you with more relevant and targeted marketing, including from our partners. We do this in several channels, for example on our websites and in social media.

Cookie overview

In addition to cookies, we use pixels and scripts from third parties. These are snippets of code that allow us to analyse your usage across social media and our channels, and we use this to give you more relevant marketing.
You can choose which categories of cookies we can use.
Turn cookies on and off

Questions and complaints

If you think we are violating privacy rules or you are unhappy with how your enquiry was handled, please contact us so that we can provide answers and clear up any misunderstandings.

Contact information

If you have any questions about this privacy policy or our processing of your personal data, please email the data protection officer at the bank or company..

Complaints to the Norwegian Data Protection Authority

You also have the right to lodge complaints with the Norwegian Data Protection Authority. Information about this can be found on the Norwegian Data Protection Authority's website.

Changes to the Privacy Policy

We need to update the Privacy Policy at regular intervals to provide you with the correct information about how we process your personal data.

Overview of changes

The following provides an overview of changes made to the privacy policy.

Change	Date

Describe the purposes such that it is easier for you to understand how we process your personal data. Simplified language.	12 June 2025
Adjustments to information about disclosing personal data.	1 October 2024
Adjustments to wording, changes to the layout of information, and addition of individual purposes and areas of use for personal data in line with business development.	16 May 2024
Necessary adjustments and clarifications in line with the development of our services, products and websites, and in line with legal developments.	28 August 2023
Necessary adjustments and clarifications in line with the development of our services, products and websites.	27 March 2023
Necessary adjustments and clarifications in line with the development of our services, products and websites.	17 June 2022