DNB’s privacy protection policy statement

DNB

Table of contents

How DNB collects and uses personal data

New privacy protection statement in the DNB Group as of 25 May 2018

The General Data Protection Regulation (GDPR), a new regulation protecting personal privacy, will enter into force in Europe on 25 May 2018. The regulation, together with a new Norwegian Personal Data Act, will come into force in Norway on 1 July 2018 at the earliest. This means that some of your new rights under the GDPR which are discussed here, will enter into force a little later in Norway than elsewhere in Europe.

In DNB, we take the security of your personal data seriously, which means that it is safe for you to use the products and services we offer. As an international financial services group we have a duty of confidentiality and will handle your personal data in accordance with prevailing data protection legislation.

The controller in the DNB Group will be a subsidiary of DNB ASA in or outside Norway which processes personal data about you because you are, for example, a customer of the entity in question. Enter the link below to see the companies in the DNB Group and find more information as well as contact details (https://www.dnb.no/portalfront/nedlast/en/about-us/juridisk-struktur-dnb.pdf).

This privacy protection statement contains information you are entitled to receive when data about you is collected, for instance from our website, and general information about how we process personal data.

The word “you” in this statement refers to you as a customer, potential customer, employee of our customer or another relevant party, such as a beneficial owner, authorised representative, corporate card holder or another associated party.

This privacy protection statement was updated in June 2018 (version 2018.06)

The types of personal data we collect

Types of personal data

Examples of the types of personal data DNB may collect are specified below. Please note that the type of personal data that is collected will depend on the product or service we are providing for you as a customer.

- **Identification information**: national identity number and name. We are required to obtain documentation verifying this information, for example a copy of your identification such as a passport, driver's licence or the like.

- **Contact information**: telephone number and address(es), including your postal address, and your country of domicile if the address is outside Norway.

- **Financial information**: customer and product agreements, transaction data, credit history and insurance history.

- **Statutory information**: country of domicile for tax purposes or foreign tax identification number as well as information that is necessary for ensuring basic knowledge of customers and for combating money laundering.

- **Special categories of data**: for example health information for certain insurance products offered by DNB's insurance companies and information about union membership in connection with some types of loan products.

Sources from which we gather your personal data

From you

Most of the personal data DNB registers will be collected directly from you as a customer, for instance when we process applications for loans or other products or you use our services in some other manner.

From third parties

To be able to offer you services and comply with statutory requirements, DNB will also gather personal data from third parties. In connection with outgoing payments, for example, we may collect information from payers, shops, banks, payment service providers and others.

Examples of such sources of information include:

- publicly available sources and other external sources/registers managed by public authorities (e.g. the National Registry and registers with the tax authorities)
- company registers
- law enforcement authorities etc.(e.g. the police, financial investigation units, etc.)
- sanction lists (kept by international organisations like the EU and the UN or national organisations like the Office of Foreign Assets Control (OFAC))
- social media
- agents and distributors
- records kept by credit agencies and other commercial entities that provide information about, for example, beneficial owners and politically exposed persons etc.

In some cases, when you give DNB authorisation to do so, we will also collect health data from healthcare institutions.

From cookies (information capsules)

When you visit one of DNB's websites (e.g. www.dnb.no or m.dnb.no), we register various types of information about you in a "cookie" (information capsule). A cookie is a small file that is stored locally on your PC. It is not harmful and cannot contain viruses or programmes. What it does is to store information from our website, for instance when you last visited it or the data you entered in an order form. It is a cookie that enables our website to remember which language you prefer or how you logged on last time and make these your default settings. All data traffic between your browser and our servers is encrypted and is stored in accordance with our strict data security requirements.

Information registered about you as a user

When you visit DNB online, we register different types of data about you as a user. According to section 2-7b of the Norwegian Electronic Communications Act you must be informed of which data will be processed, the purpose of the processing and who will process it. Your consent is required in this connection.

The registered data can, for example, be:

- your location, using an IP address, location data or the like
- your web behaviour, e.g. which pages you visit and how often, or which products you order
- technical data about your browser and operating system

Purposes of and use of data gathered through our website

Data about your web behaviour is used for several different purposes:

Analytical purposes

To enable us to learn from your and other users' behaviour, we use a system called Webtrends Analytics to analyse data as a basis for improving the website's functionality and contents and the user experience. Data from Webtrends' information capsules, such as IP addresses, is anonymised and stored on Webtrends' servers in the US. Anonymisation means that none of the information can be traced back to you. The following information capsules are used for this purpose:

- WT_FPC – randomly generated identifier for your visit and your browser
- ACOOKIE – sends information about your visit to WT_FPC
- UTAG_MAIN – randomly generated identifier for your visit and your browser

We use a tag management system called Tealium IQ to manage the tools we use for analysis and marketing. No data is stored there.

Technical purposes

To make our website as stable as possible, we distribute the web traffic among multiple servers through a traffic distribution "junction". The following information capsule is used for this purpose:

- IV_JCT

Customisation

To ensure that the contents of the webpage are as relevant as possible for you, we use information capsules containing data about factors like language, segment and your digital unit. In some cases, the data we gather in connection with website use will be combined with other information about your customer relationship with DNB.

The following information capsules are used for this purpose:

- Sp
- portal scriptable
- portal persistent
- dnbnorsession
- deviceinfo
- NorSegdOpSitesSessionID

Marketing

We use information capsules issued by third parties to give you more relevant advertisements and offers in other channels. This data is based on contents and pages on our website that you have visited. The data in the information capsules is aggregated before being sent to third parties. This involves combining and anonymising the information so third parties cannot access personal data or other information that could identify you as a user of our webpages. The Norwegian Personal Data Act, the EU's General Data Protection Regulation and the Norwegian Marketing Control Act regulate the use of customer data for this purpose. The third-party sources we use are Google (https://www.google.com/), YouTube (https://www.youtube.com/), Facebook(https://www.facebook.com/), Adform (https://site.adform.com/) and DoubleClick.net (https://www.doubleclickbygoogle.com/).

The following information capsules from third parties are used for this purpose:

- Id
- NID
- PREF
- YSC
- VISITOR_INFO1_LIVE

Read more about how Google uses the different information capsules listed above. (https://translate.google.no/translate?hl=no&sl=en&tl=no&u=https%3A%2F%2Fpolicies.google.com%2Ftechnologies%2Fcookies&anno=2)

Browser settings for information capsule use

Enabling the use of information capsules will give you a more relevant user experience when you visit websites. You can change this by changing the settings in your browser. Check WikiHow (https://m.wikihow.com/Disable-Cookies) for instructions on how you can delete or disable information capsules.

Recording of telephone conversations and storage of electronic communication

DNB is required by law (e.g. according to the Norwegian Securities Trading Act) to record telephone conversations and store electronic communication in which you, as a customer, are given advice about loans, saving, investments or similar services. DNB records all conversations you have with advisers or brokers, e.g. in Markets, DNB Private Banking or DNB Asset Management, who provide the aforementioned services.

DNB may listen to conversations and review other electronic communication for quality control purposes.

Storage time:
Recordings may only be used when you or we have a need to document the advice given. Recordings are stored for at least five years and are deleted when DNB no longer has legitimate grounds for continuing to store them.

Disclosure to others:
DNB can be ordered to disclose information to public authorities and others entitled to demand disclosure according to law. In addition, information may be disclosed to the Financial Complaints Board, for instance in connection with the consideration of complaints.

Right to play recordings:
Requests to inspect documentation concerning investment services and listen to recordings should be directed in writing to: DNB Bank ASA, Kort- og bankreklamasjoner, Beddingen 16, 7469 Trondheim. You can make such requests for up to five years after the conversation was recorded. When you ask for a recording to be played, you must specify when the conversation was recorded and from which telephone number.

Video surveillance

To prevent and detect criminal acts, buildings managed or leased by DNB are monitored by surveillance cameras.

As a rule, surveillance videos recorded by security cameras that DNB controls are stored for seven days after the recording date. Surveillance footage of bank offices, branch offices, ATMs and payment terminals linked to in-store banking outlets is stored for 90 days. These storage periods apply except in cases where the surveillance video is given to the police or DNB has the right to use the video recordings for another purpose.

Purposes for which personal data is used

Customer administration

DNB will use your personal data to meet its obligations when executing orders for you and according to service agreements with you, and in connection with customer administration and invoicing.

When entering into agreements with you and during the term of such agreements, DNB will register information about you and other persons involved in the contractual relationship, e.g. authorised users. DNB will also register information about individuals with whom it has declined to enter into agreements as a basis for informing the individuals that their application was declined and to be able to document the circumstances later on, if necessary.

Marketing

The financial institutions in the DNB Group are entitled to share neutral information about you among them and use it for marketing purposes without obtaining your consent, within the limits set by the Norwegian Marketing Act. Such information includes name, contact details, date of birth, and the services and/or products you have subscribed to. The Group's investment firm, DNB Markets, and asset management firm, DNB Asset Management, are subject to strict confidentiality rules that limit the extent to which personal data can be shared between these entities and the bank.

DNB is entitled to process personal data for marketing purposes when this is necessary to pursue a legitimate interest that overrides your right to protection of personal privacy. Your consent is required for the marketing of products and services in categories other than those you have agreed with DNB if this involves using other than neutral customer data.

Profiling

By "profiling" we mean all forms of automated processing of personal data for the purpose of evaluating characteristics associated with you. This includes, for example, analysing or predicting elements of your financial situation, your personal preferences or transaction patterns.

DNB uses profiling when preparing and carrying out advertising campaigns, for customer follow-up and when preparing offers for products. The bank has a legitimate interest to use profiling, for example when performing a customer analysis for marketing purposes or monitoring transactions to enable the detection of fraud.

Group customer register

The DNB Group has a shared customer register. The data in the register is used to manage customer relationships and coordinate offers of services and advice from the different companies in the Group.

The group-wide customer register will contain neutral information about you like your name, date of birth, address and other contact information, as well as information about the companies in the Group you are a customer of, and the services and products for which you have entered into agreements. Your national identity number may be shared and registered in a group-wide customer register when the purpose is administration of the customer relationship.

Security

DNB has implemented technical and organisational security measures to protect your personal data. DNB continuously seeks to ensure that your personal data is protected against loss, destruction, corruption or unauthorised access. Our security framework is updated regularly in line with technological developments.

In addition, DNB is permitted to process personal data to pursue the legitimate interest of securing the Group's assets, for instance in connection with logons to servers, the operation of infrastructure, firewalls, access controls and video surveillance.

Risk classification of customers and credit portfolios

DNB will process credit information and other personal data in accordance with the provisions of the Norwegian Financial Institutions Act and Securities Trading Act. This processing takes place in connection with the establishment of your customer relationship, determining which products and services are suitable for you and the use of systems to calculate capital adequacy requirements for credit risk. The internal measurement systems include DNB's models, work and decision-making processes for approving and managing credit, control mechanisms, IT systems and internal guidelines for classifying and quantifying the Group's credit risk and other relevant risk. The personal data used for this purpose is obtained from credit agencies.

Prevention and detection of criminal acts

DNB is permitted to process personal data for the purpose of preventing, detecting, investigating and handling fraud and other criminal acts. In such cases, DNB may need to gather information and disclose it to other banks and financial institutions, the police and other public authorities. The collected information may be stored for up to ten years after it is registered. DNB will process personal

data to fulfil its obligation to investigate and report suspicious transactions in accordance with the Norwegian Money Laundering Act. DNB has a statutory obligation to report suspicious information and transactions to the Financial Investigation Unit in ØKOKRIM (the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime). According to the Norwegian Personal Data Act and the Money Laundering Act, you are not entitled to inspect certain information registered by DNB in this connection as long as an investigation is still ongoing.

DNB will otherwise process personal data to the extent this is required or permitted by law or when you have given your consent. In addition, DNB is permitted to process personal data for the purpose of preventing and detecting criminal acts if this is necessary to protect a legitimate interest that overrides the right to protection of your personal privacy.

Customer authentication using electronic services

When you use DNB's electronic services, DNB is permitted to register your user behaviour and user environment and any deviations from these, identify the computer or mobile device you use to carry out the banking service, the state of the computer/unit etc. DNB will use this data to make sure that the right person is using the service in question. DNB may also use the data in a risk assessment to adjust the authentication method that you have to use for the service.

Analysis and development of new services

In connection with the improvement of existing services or development of new ones, DNB may collect information for the purpose of analysing how you, as a customer, use DNB's services.

In some cases, DNB is permitted to process personal data for the legitimate purpose of analysing usage patterns to identify potential demand for new products and services, improving existing products and services and performing tests in connection with development.

Automated decisions

In some cases, we can use automated decisions when this is permitted by law and you have explicitly consented to this, or if it is necessary for the performance of an agreement, e.g. automated credit decisions in our online channels. You may, at any time, request manual processing instead, state your opinion or contest a decision that is exclusively based on automated processing, including profiling, if such a decision could have legal or other significant consequences for you.

When we use automated decision-making processes, we will give you additional information about the underlying logic that is used and the consequences it can have for you.

Who we are permitted to share your personal data with

Third parties

In some cases, we have legitimate grounds for sharing your personal data with other parties, such as the authorities, companies in the DNB Group, suppliers, providers of payment services and business partners. Before disclosing such information we always check to ensure that we comply with relevant rules regarding the duty of confidentiality in the financial and securities sectors.

We sometimes need to disclose information about you when we deliver services and products. If, for example, you have instructed us to transfer money or securities, we need to disclose certain information to carry out the transfer.

When DNB outsources tasks that call for a service provider to process personal data on behalf of DNB rather than for its own purposes, the service provider will normally be a data processor. In such cases DNB is required to enter into a data processor agreement with the service provider. This applies irrespective of whether DNB uses data processors in Norway or another country in the EEA.

The DNB Group uses data processors (e.g. providers of IT services) to gather, store or otherwise process personal data on its behalf. In such cases, DNB will enter into agreements with data processors to ensure that such processing meets the requirements stipulated in privacy protection regulations and DNB's requirements for processing personal data. The use of data processors is not regarded as disclosure of personal data.

DNB currently uses the following types of data processors:

- software providers
- cloud solution providers
- distributors and agents
- sourcing partners
- consultants

Transfer of personal data to countries outside the EEA

All transfers of personal data from DNB to a service provider are conditional on a data processor agreement between DNB and the service provider. This applies irrespective of whether DNB uses data processors in Norway or another country in the EEA.

In some cases, DNB transfers personal data to organisations in countries outside the EEA, e.g. providers of IT services or other data processors. Such transfers are only permitted when the data controller or data processor has issued the required guarantees and on the condition that the individuals are guaranteed enforceable, effective rights.

According to the GDPR, there must be a legitimate reason for such transfers, and some of the following conditions must be met:

- The European Commission has determined that there is an adequate level of protection in the country in question.
- Other suitable security measures have been implemented and/or the data processor has given the necessary guarantees that personal data will be processed in a secure manner, e.g. by means of standard contracts (the EU's standard clauses) approved by the European Commission, or the data processor has valid, binding corporate rules (BCR).
- It is an exception, under special circumstances, e.g. in order to perform an agreement with you or when you have consented to the transfer in question.

Legitimate grounds for processing

DNB must have legitimate grounds for processing personal data. The most important legitimate grounds are listed below.

Necessary to perform an agreement with you

DNB primarily processes personal data for the purposes of customer administration, provision of financial advice, invoicing and the provision of banking, insurance and financing services in accordance with your agreements with DNB.

Statutory obligations

DNB processes personal data to meet its obligations according to laws, regulations and the decisions of the authorities.

Examples of processing for the purpose of fulfilling statutory obligations:

- preventing and detecting criminal acts such as money laundering, terrorist financing and fraud
- monitoring sanctions
- to meet accounting requirements
- to submit reports to the tax authorities, the police, execution and enforcement authorities and supervisory authorities
- to meet requirements and obligations related to payment services
- to meet other obligations according to legislation concerning specific services or products such as securities, mutual funds, collateral, insurance or home mortgages

Legitimate interest

DNB is permitted to process personal data when this is necessary to protect a legitimate interest that outweighs an individual's right to protection of personal privacy. The legitimate interest must be legal, predefined, real and justified by business operations.

Examples of processing based on legitimate interests:

- marketing in connection with ongoing contractual relationships
- customer analyses based on profiling for marketing purposes
- transaction monitoring to detect criminal acts

Consent

If there is no other statutory basis for processing, DNB's processing of personal data must be based on your freely-given, specific consent. You will always be asked to give your consent if personal data categorised as sensitive (e.g. information about your health, religious beliefs, sexual orientation, ethnicity etc.) needs to be processed.

Even if you have given DNB consent, you can withdraw it at any time. If you withdraw your consent, the processing will be stopped and, if further storage of the data in question is conditional on your consent, it will be deleted. Information about the purpose, processing activities and your right to

withdraw your consent will be provided when you are asked to give DNB your consent through different channels.

Your rights

Access to information and data portability

A request for data access gives you the right to inspect the data that we have stored about you. This applies to data you have provided yourself, data we have obtained from external sources and information about the processing of this data.

Your right to data access does not extend to internal assessments and similar internal data created by data controllers on the basis of personal data you have given us. The same applies to certain personal data we have gathered to fulfil statutory obligations, such anti-money laundering obligations. Please check the online bank for detailed information and historical data about the products and services you use. If you do not subscribe to our online banking services, you will have received this information in our regular dispatches by post.

Data access report
The data access report provides you with an overview of your registered personal data, description of the types of information being processed and details of how we process the data.

» Order data access report through the following link (https://www.dnb.no/en/personal/customer-service/gdpr/logginn-data-access.html)

Data portability is your right to receive personal data you have given us. The information must be sent in a machine-readable format. This applies to information you have given us directly, given us consent to collect or that is required to perform an agreement. More detailed information and historical data about your products and services can also be downloaded from the online bank.

Data portability report
The portability report gives you an overview of what information you have given us directly, based on your agreement or in order to fulfill a deal in a machine-readable format.

» Order portability report through the following link (https://www.dnb.no/en/personal/customer-service/gdpr/logginn-data-portability.html)

Current or former DNB-employees

If you are or have been an employee of DNB and wish to request a copy of your personal data in DNB's records, please contact HR administration at hrsupport@dnb.no, and specify the telephone number on which you want to be contacted.

Objection to processing

You have the right to object to any processing of your personal data that is carried out to protect legitimate interests unless such interests take priority over your basic rights or freedoms.

In cases where our legitimate interest is the basis for processing your personal data and the data is used for direct marketing and profiling related to such marketing, you always have the right to object to the processing.

The right to erasure of personal data

As long as you have one or more active agreements with us, we will need to store personal data about you that is linked to these agreements. After an agreement expires, the personal data will be stored for a while to ensure that you get the best possible customer service. The other reasons for storing data after agreements expire are to meet our statutory obligation to store data and to defend ourselves against any legal claims. After the set storage period your personal data will be deleted. We are, for example, permitted to store personal data linked to a home mortgage for five years after the loan is repaid.

DNB is required by law to store certain data, including personal data, for purposes such as accounting, tax reporting and reporting to the authorities. This data will also be deleted automatically, but normally after a longer period of time. It should be underlined that this personal data will only be used for the above-mentioned purposes and access to it is thus strictly limited. If all of your agreements with us are cancelled, we will also terminate your customer relationship.

If you find that DNB is storing your personal data unlawfully, you are entitled to instruct us to delete it ("the right to be forgotten").

Correction of incorrect personal data

If the data we have about you is inaccurate or incomplete, you are entitled to request rectification of the data within the limits that follow from legislation.

Limits on processing of personal data

If you contest the accuracy of data we have registered about you, or have exercised your right to contest the legality of processing such data, you can ask us to limit processing to simply storing the data. In such event, processing will be limited to storage until the data has been corrected or it has been determined that our legitimate interests take precedence over your interests in this connection.

In some cases you do not have the right to delete data we have registered about you, though you can ask us to limit the processing of such data to just storing it. If processing of your personal data is necessary to present a legal claim, you can also demand that any other processing of the data is to be limited to storage. We are only permitted to process your personal data for other purposes when this is necessary to make a legal claim or if you have given your consent.

If you choose to impose limits on DNB's processing of your personal data it can result in products and services no longer being available to you. Please feel free to contact us for more information about the consequences such restrictions can have for your customer relationship.

Contact information

Questions and complaints

For customers of DNB companies in Norway:

If you have any questions about this privacy protection statement or about how DNB handles your personal data, you can contact DNB's customer service centre 24 hours a day by means of the chat function in the Internet bank, on telephone number +47 915 04800 or via dnb.no. Choose the following link if you want to send a complaint to DNB electronically (https://www.dnb.no/privat/kundeservice/klage-og-reklamasjon.html). If you want, you can also send your complaint directly to the Norwegian Data Protection Authority. For more information, please see the Data Protection Authority's website (https://www.datatilsynet.no/).. DNB also has a data protection officer who can be contacted by email: personvernombudet@dnb.no or by post: DNB, c/o Personvernombud, P. O. Box 1600 Sentrum, 0021 Oslo, Norway.

For customers of DNB companies outside Norway:

If you have questions about how DNB processes your personal data, or about this privacy protection statement, please contact your international DNB office (https://www.dnb.no/en/about-us/global-network.html). Your international DNB office will also be able to give you information about the local data protection officer. You can also send your complaint directly to the local data protection authority. Check your local data protection authority's webpage for information about this.

Changes

In DNB, we continuously seek to improve and develop our services, products and websites. In the event of any changes of the rules for processing personal data, changes of our services and products or other changes that affect this personal privacy statement, the information in this statement will be changed correspondingly.

Change log

A section about profiling for processing purposes was added	See "Profiling"
A section about the right to limit processing was added	See "Limits on processing of personal data"
Minor adjustments and refinements	Throughout the document