Danske Bank A/S Norway Privacy Notice for All Individuals

This privacy notice was last updated on 1 November 2024

1. Introduction

This privacy notice applies to the processing of personal data by the Norwegian branch of Danske Bank A/S ('Danske Bank').

Data controllers – Danske Bank is the data controller for processing of personal data described in this privacy notice.

Contact details – Danske Bank A/S, Danish CVR. no. 61126228 (Erhvervs- og Selskabsstyrelsen) Bernstorffsgade 40, DK-1577 København V,

Danske Bank Norwegian branch Company Reg NO; 977074010 (Foretaksregisteret), Søndre Gate 15, 7011 Trondheim.

More information about the data controllers and the Norwegian branch is available on the respective websites www.danskebank.dk and www.danskebank.no.
In the course of our business, we process information about you (personal data).

This privacy notice applies to private customers, potential private customers, sole trader customers, guarantors, pledgers and where applicable other individuals connected to a customer such as partner, spouse, guardians, authorized representatives, holders of a power of attorney, employees or owners of a corporate customer, other third parties involved in transactions and other individuals with whom we interact and collaborate with.

This privacy notice sets out how and why Danske Bank processes your personal data and protects your privacy rights

2. What personal data do we collect and process

Depending on your relation with the bank and depending on the services or products we are offering, we process different kinds of personal data, including

- Personal details including your name, signature, social security number or other national ID number, citizenship, gender, country of residence, picture, 3D scan and identification documentation such as copies of your passport, driver's licence and birth certificate,
- Contact information, including your address, telephone number and email address
- Financial information, including details about your income, assets, debt, credit rating and insurances
- Information about collateral, including market value, energy data and environmental aspects
- Information about your education, profession, work knowledge and experience
- Information about your investment targets
- Information about your family and household
- Information if you as our private customer also is an entrepreneur
- Details about the services and products we provide to you, including amongst others accounts, cards, loans, credits, etc.,
- Transaction data
- How you use our services and products and your preferences towards them
- Digital information related to your use of our websites, platforms and digital applications, including traffic data, location data, behavioural data and other communication data
- Information related to the devices you use to access our websites as well as technical information, including the type of device and operating system
- Information provided by you about your preferences for various types of marketing and events
- Information about your visits to our premises
- Conversations with you over telephone, Teams or other online meeting tools, and
- Other information received through our different communication channels

Our ability to offer the best advice and solutions for you very much depends on how well we know you. Consequently, it is important that the information you provide is correct and accurate and that you keep us updated on any changes.

3. What we use your personal data for

We process data about you to provide the best advice and solutions, keep your finances safe and fulfil our agreements with you, protect you and Danske Bank against fraud, for data security and to comply with applicable regulations.

We process personal data to provide you, or the customer of us you are related to, with the financial services or products that has been requested, including

- Payment services
- Accounts
- Card services
- Loans and credit
- Digital banking solutions
- Investment services and advice
- Insurance and pension services

We process personal data for the following purposes

- To be able to offer you our products and services
- For onboarding purposes in relation to identification and verification for anti-money laundering and combating terrorist financing purposes
- Customer service and managing the customer relationship, including advice, administration, credit assessment, recovering of outstanding debt, handling of complaints and to make information available to service providers who are authorized to request your information
- Communicating with you about your products and services for legal, regulatory and servicing purposes
- To improve, develop and manage our products and services and setting fees and prices for our products and services, including use of data analytics and statistics to improve products and services and to test our systems
- For marketing of our services and products, including marketing on behalf of other entities in the Danske Bank Group or our partners, if we have your permission or if we have legal basis, such as the Norwegian marketing act section 15. We use cookies and similar technology on our website, including for marketing via digital channels and social media platforms. We refer to our cookie policy at https://danskebank.no/behandling-av-opplysninger-og-cookies for further information
- To comply with applicable law and for other regulatory and administrative purposes, including identification and verification according to anti-money laundering legislation, risk management, and prevention and detection of money laundering, terrorist financing, fraud and other types of financial crime. In relation to anti-money laundering and combating terrorist financing, identification data is collected at regular intervals during your agreement with us as required by law
- For security purposes, including use of video surveillance of ATMs, entrances to our branches and other premises

4. What is our legal basis for processing your personal data?

We must have a legal basis (lawful reason) to process your personal data. The legal basis will be one of the following:

- You have granted us consent to use your personal data for a specific purpose, cf. the General Data Protection Regulation (GDPR) art. 6.1(a),

- You have made or you are considering making an agreement with us for a service or product, cf. GDPR art. 6.1(b),
- To comply with a legal obligation, cf. GDPR art. 6.1(c), for example, in accordance with
  - The Norwegian Anti-Money Laundering Act (Hvitvaskingsloven)
  - The Norwegian Financial Agreement Act (Finansavtaleloven)
  - The Norwegian Financial Institution Act (Finansforetaksloven)
  - The Norwegian Tax Management Act (Skatteforvaltningsloven)
  - The Norwegian Book-keeping Act (Bokføringsloven)
  - The Norwegian Securities Trading Act (Verdipapirhandelloven)
  - The Norwegian Debt Information Act (Gjeldsinformasjonsloven)
  - The Norwegian Marketing Act (markedsføringsloven)
  - The General Data Protection Regulation (GDPR) and the Danish and the Norwegian Data Protection Act (Personopplysningsloven)
  - The Danish Financial Business Act (Lov om finansiell virksomhet)
- It is necessary to pursue a legitimate interest of Danske Bank, cf. GDPR art. 6.1(f). For example, this may be:
  - For documentation and security purposes,
  - To prevent and detect money laundering or terrorist financing,
  - To prevent and detect fraud, abuse and loss,
  - To strengthen IT and payment security and
  - For direct marketing purposes.

We also use legitimate interest as legal basis, when we process data about you when you are not the customer of ours but interact with us due to the relation you have to one of our customers. We will only do so if our legitimate interest in each case is not overridden by your interests or rights and freedoms.

5. Special categories of personal data

Some of the information we hold about you might be special categories of personal data (also known as sensitive personal data).

Types of special categories of personal data

In particular, we may process the following types of special categories of personal data:

- trade union membership information,
- information about your health and your genetic background, e.g. inherited health qualities,
- biometric data, e.g. via facial recognition technology,
- information about your religious or philosophical beliefs, and
- information about your political opinions.

We also process special categories of personal data that may appear in budget information you give us and transactions you ask us to initiate or that you execute through our digital services.

Purposes for processing special categories of personal data

We will only process special categories of personal data when we need to, including

- for the purposes of the product or service we provide to you,
- to give you discounts related to e.g. trade union memberships,
- for identification and verification,
- for prevention and detection of money laundering, terror financing and other types of crime, including for fraud prevention and detection purposes, and

- to comply with legal requirements that apply to us as a financial institution.

Legal basis for processing special categories of personal data

Our processing of your special categories of personal data can be on the legal basis of

- your explicit consent, cf. GDPR art. 6.1(a) and 9.2(a),
- for reasons of establishment, exercise or defence of legal claims, cf. art 6.1(f) and 9.2(f); or
- for reasons of substantial public interest, cf. GDPR art. 6.1(c) or 6.1(f) and art. 9.2(g).

6. How do we collect the information we hold about you

Personal data collected from you

We collect information directly from you or by observing your actions, including when you

- Fill out applications and other forms for ordering services and products,
- Submit specific documents to us,
- Participate in meetings with us, e.g. with your advisor,
- Talk to us on the phone,
- Use our website, mobile applications, products and services,
- Participate in our customer surveys or promotions organised by us, and
- Communicate with us via letter, electronic means, including e-mails, or social media.

Voice recordings

When you call us or when we call you at your request or to follow up on your inquiry, conversations will be recorded and stored if required by legal obligations or if you give your consent. If we talk with you about investment services, we are legally obliged to record and store our telephone conversation, Teams call or similar.

Personal data collected from third parties

We collect data from third parties, including from:

- Shops, banks, payment and services providers when you use your credit or payment cards, Danske eBanking or other payment services. We process the data to execute payments and prepare account statements, payment summaries and the like.
- If you have a joint account with someone, we may collect information about you and your joint account from your co-account holder.
- The Norwegian National Population Register (Folkeregisteret), maintained by the Norwegian Tax Administration (Skatteetaten), the Norwegian Register of Business Enterprises (Foretaksregisteret) and other publicly accessible sources and registers. Sometimes we collect these data via other third parties. We process the data, for e.g. identification and verification purposes and to check data accuracy.
- Credit rating agencies and payment remarks registers (for instance Bisnode and Dun & Bradstreet). We process the data to perform credit assessments. We update the data regularly.
- Other entities in the Danske Bank Group if we have your consent, e.g. to provide you with better customized products and services.
- Other entities within Danske Bank Group if applicable law allow or require us to collect the information, e.g. if it is necessary to comply with legal requirements on group-based management, control and/or reporting, or collection of notifications to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) in accordance with the Anti-Money Laundering Act.
- External business partners (including correspondent banks, other banks and other legal entities) if we have your consent or if permitted under existing legislation, for example to provide you with a service or product provided by an

external business partner you have signed up for, to enable our customers to use banking services abroad, or to prevent and detect money laundering, fraud, abuse and loss.
- The customer you have a connection with.

7. Third parties that we share your personal data with

We will keep your information confidential but we may share it with third parties (who also have to keep it secure and confidential) in the following situations

- Other entities in the Danske Bank Group if we have your consent, e.g. to provide you with better customized products and services
- Other entities within Danske Bank Group if existing legislation allow or require us to share the information, e.g. if it is necessary to comply with legal requirements on group-based management, control and/or reporting requirements, or sharing of notifications to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) in accordance with the Norwegian anti-money laundering act
- If you have asked us to transfer an amount to others, we disclose data about you that is necessary to identify you and fulfil the agreement
- Service providers who are authorized as an account information service, payment initiation service, or card-based payment instrument provider, if you (or someone who via our online services can view information about your accounts or initiate payments on your behalf) request such a service provider to receive information about you.
- Guarantors, pledgers, individuals holding a power of attorney, lawyers, accountants or others you have authorised us to share the information with
- If you have a joint account with someone, we may share your information with your co-account holder.
- External business partners (including correspondent banks, other banks and other legal entities) if we have your consent or if permitted under applicable law, for example to provide you with a service or product you have ordered, and which is provided by an external business partner, or to prevent and detect money laundering, terrorist financing, fraud, abuse and loss
- Our suppliers, including lawyers, accountants and consultants
- Data processors, such as providers of payment services or IT services. Data processors may be located both inside and outside the EEA, such as for example Vipps Mobilepay AS headquartered in Norway, and Infosys located in India.
- Public authorities as required by law or according to court orders or requests from the police, the bailiff or other authorities. This could include the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) in accordance with the Norwegian Anti-Money Laundering Act, the Norwegian Tax Authorities in accordance with the Norwegian Tax legislation, the Norwegian Central Bank (Norges Bank) for statistical and other purposes and overseas tax authorities for FATCA/CRS reporting purposes, the Norwegian Foreign Ministry or the Norwegian Directorate for Export Controls pursuant to the sanction act with underlying regulations
- Regulators, e.g., the Danish and the Norwegian Financial Supervisory Authority (DK: Finanstilsynet NO: Finanstilsynet), law enforcement agencies and authorities in Norway and in other countries, including outside the EU and the EEA, in connection with their duties
- Credit rating agencies. If you default on your obligations to Danske Bank, we may report you to credit rating agencies and/or warning registers in accordance with applicable law (for instance Bisnode and Dun & Bradstreet).
- For social and economic research or statistics purposes, where it is in the public interest
- In connection with transactions (including purchase or mergers) which results in that our business, in whole or in part, are transferred to another company, we may share your data to the extent necessary to complete the transfer and your customer relationship within the framework of the legal requirements we need to comply with

8. Transfers outside the EU and the EEA and international organisations

Some third parties that we share personal data with may be located outside the EU and the EEA, including the UK, the US, Australia, Canada and India.

When Danske Bank transfer your personal data to third parties outside the EU and the EEA, we ensure that your personal data and data protection rights are subject to appropriate safeguards through

- Ensuring that there is an adequacy decision by the European Commission
- When transferring to the USA, ensure that the transfer is made to certified parties under the EU-US Data Privacy Framework, in accordance with GDPR Article 45
- Transfer your personal data to parties outside the EU/EEA based on the specific exemptions set out in GDPR art. 49, for example in GDPR art. 49(1)(e), if the transfer is necessary for our establishment, exercise or defence of a legal claim, or
- Using standard contracts approved by the European Commission or the Danish or Norwegian Data Protection Agency or internal rules for data transfers in multinational companies, also called binding corporate rules

You can get a copy of the standard contract by contacting us (see contact details in Section 13).

9. Profiling and automated decisions

Profiling

Profiling is a form of automated processing of your personal data to evaluate certain personal aspects relating to you to analyse or predict aspects concerning for example, your economic situation, personal preferences, interests, reliability, behaviour, location or movements.

We use profiling and data modelling to be able to offer you specific services and products that meet your preferences, prevent money laundering, determine prices of certain services and products, prevent and detect fraud and risk of fraud, evaluate the likelihood of default, value assets and for marketing purposes.

Automated decision-making

With automated decision making, we use our systems to make decisions without any human involvement based on the data we have about you. Depending on the specific decision, we might also use information from public registers and other public sources.

We use automated decisions for example to approve loans or credit cards, to prevent and detect money laundering and to prevent and detect fraud. Automated decision making helps us make sure that our decisions are quick, fair, efficient and correct, based on what we know.

In relation to loans and credit cards, we consider information about your income, your expenses and how well you have kept up on payments in the past. This will be used to work out the amount we can lend you.

In relation to fraud prevention and protection, we do our best to protect you and your account against criminal or fraudulent activity by monitoring your transactions (payments to and from your account) to identify unusual transactions (for example, payments you would not normally make, or that are made at an unusual time or location). This may stop us from completing a payment that is likely to be fraudulent.

You have rights relating to automated decision-making. You can obtain information about how an automated decision was made. You can ask for a manual review of any automated decision. Please see section 11 on 'Your rights' and 'Automated decision making'.

10. How long do we store your personal data?

We keep your data for as long as it is necessary for the purpose for which your data were registered and used, and only as long as we have a lawful basis to process the personal data.

When your business connection with us has terminated, we normally keep your data for a time period in accordance with legal obligations and requirements and/or Danske Banks legitimate interest.

We normally keep your data for up to a further 13 years after our business connection has terminated, the maximum general limitation period according to the Norwegian Limitation Act § 3, cf. § 10, to ensure that the bank can provide relevant documentation related to a dispute until the claim is time-barred.

Our legal obligations to keep data is inter alia set out in the Bookkeeping Act, the Anti-Money Laundering Act, the Securities Trading Act and requirements from the Financial Supervisory Authority.
In certain circumstances, we keep your information for a longer period of time if we have a legitimate interest to do so. This is the case for example

- If your personal information form part of our calculation of our capital requirements, then we may keep your information for up to 20 years
- If the statute of limitation is 3 years and it may be prolonged by up to 10 years, we may keep your data in accordance with Danske Banks legitimate interest for up to 13 years, cf. the Norwegian Limitation Act § 3, cf. § 10, and
- If the statute of limitation is 10 years, then we may keep your data in accordance with Danske Banks legitimate interest for up to 10 years, and
- If required to due to other regulatory requirements

If you as a potential new customer have asked for an offer for a loan or another product or service but refuses, is rejected and/or cancelled and do not become a customer, your personal data will be stored for a period of minimum six months, and may for some purposes be stored longer, to comply with legal obligations, and/or in accordance with Danske Banks legitimate interest.

11. Your rights

Your rights in relation to personal data are described below. To exercise your rights, you can for example

- Make a request online at https://danskebank.no/privat/skjemaer/gdpr-formular-en
- Send a message in the digital bank
- Contact us via our main telephone number 987 08540, or
- If you have a personal advisor, contact your advisor directly

See section 13 for more information on how to contact Danske Bank about data protection.

Right to access your personal data

You can request access to the personal data we process, where it comes from and what we use it for. You can obtain information about for how long we store your data and about who receives data about you, to the extent that we disclose data in Norway and abroad. Your right of access may, however, be restricted by legislation, protection of other persons' privacy and consideration for our business and practices. Our know-how, trade secrets as well as internal assessments and material may also be exempt from the right of access.

You can make an access request via the mobile bank app or our webpage at https://danskebank.no/privat/skjemaer/gdpr-formular-en.

In addition to the access request, you may under the 'Profile' section of the mobile bank app, obtain a high level overview of the personal data you have given us. You will find your contact information and information you have given us about your household, income, debt and so on. You can update the information if changes have occurred in your life. You can also manage some of your consents.

Rights related to automated decision making

You can obtain information on how an automated decision was made and the effects of the decision, you can express your point of view, you can contest the decision, and you can request a manual review of any automated decision.

Right to object

In certain circumstances, you have a right to object to the processing of your personal information. This is the case for example when the processing is based on our legitimate interest.

Objection to direct marketing

You have the right to object to our use of your personal information for direct marketing purposes, including profiling that is related to such purpose.

You can always contact us and request a block concerning all types of direct marketing.

Right to rectification of your data

If data is inaccurate, you are entitled to rectification of the data. If data is incomplete, you are entitled to have the data completed, including by means of providing us a supplementary statement.

Right to erasure ('right to be forgotten')

You are entitled to have your data erased, if the data is no longer necessary in relation to the purposes for which they were collected.

There are some exemptions where we may or are required to keep your data, including

- For compliance with a legal obligation, for instance if we are obliged by law to hold your data for a certain amount of time, e.g., according to Anti-Money Laundering Act or the Bookkeeping Act. In such situations, we cannot erase your data until that time has passed
- For the performance of a task carried out in the public interest
- For establishment, exercise or defence of legal claims

Restriction of use

If you believe that the data we have registered about you is incorrect, or if you have objected to the use of the data, you may demand that we restrict the use of these data to storage. Usage will then only be restricted to storage until the correctness of the data can be established, or it can be checked whether our legitimate interests outweigh your interests.

If you are entitled to have the data we have registered about you erased, you may instead request us to restrict the use of these data to storage. If we need to use the data we have registered about you solely to assert a legal claim, you may also demand that other use of these data be restricted to storage. We may, however, be entitled to other use to assert a legal claim or if you have granted your consent to this.

Withdrawal of consent

Where consent is the legal basis for a specific processing activity, you can withdraw your consent at any given time. Please note that we will continue to use personal data about you that we have already collected, for example, to fulfil an agreement we have made with you or we are required to do so by law.

Data portability

If we use data based on your consent or as a result of an agreement, and the data processing is automated, you have a right to request the copy of the data you have provided in an electronic machine-readable format and the right to have the personal data transmitted to another controller.

12. Changes to this privacy notice

We may change or update this privacy notice on a regular basis. In case of a change, the 'last updated' date at the top of this document will be amended. If changes to how your personal data are processed will have a significant effect on you personally, we will take reasonable steps to let you know of the changes to allow you to exercise your rights (for example, to object to the processing).

13. Contact details and how Can you complain

You are always welcome to contact us if you have questions about your privacy rights and how we process personal data.

You can contact us via our main telephone number 987 08540. You are also welcome to contact your advisor directly.

You can contact our Data Protection Officer via email dpofunction@danskebank.com or by letter to Danske Bank Data Protection Officer, Postboks 4700, 5466 Trondheim..

If you are dissatisfied with how we process your personal data, and your dialogue with the Data Protection Officer has not led to a satisfactory outcome, you can contact our complaints handling unit via email klage@danskebank.no or via mail Danske Bank Klage, Postboks 4700, 5466 Trondheim.

You can also lodge a complaint to the relevant authority

The Danish Data Protection Agency – Datatilsynet, Carl Jacobsens Vej 35, DK-2500 Valby, email – dt@datatilsynet.dk

The Norwegian Data Protection Authorities – Datatilsynet, Postboks 458 Sentrum, 0105 Oslo, email; arkiv@datatilsynet.no