

# PRIVACY NOTICE FOR PRIVATE CUSTOMERS AND PRIVATE INDIVIDUALS

Danske Bank A/S, Finland Branch, Danske Invest Fund Management Ltd, Danske Mortgage Bank Plc

Effective from May 8, 2024

## 1. Introduction

This privacy notice applies to the processing of personal data by the Finnish branch of Danske Bank A/S (Danske Bank A/S, Finland Branch).

This Privacy Notice is also applicable on Danske Invest Fund Management Ltd's and Danske Mortgage Bank Plc's processing of personal data. Both companies are wholly owned subsidiaries of Danske Bank A/S.

Danske Bank A/S, Danske Invest Fund Management Ltd and Danske Mortgage Bank Plc are all separate data controllers for the processing of personal data described in this privacy notice.

### Contact details:

Danske Bank A/S, CVR no. 61126228, Bernstorffsgade 40, DK-1577 København V, DENMARK

Danske Bank A/S, Finland Branch, Business ID 1078693-2, Televisiokatu 1, 00075 DANSKE BANK

Danske Invest Fund Management Ltd, Business ID 0671602-6, Televisiokatu 1, 00075 DANSKE BANK

Danske Mortgage Bank Plc, Business ID 2825892-7, Televisiokatu 1, 00075 DANSKE BANK

More information about the data controllers and the Finnish branch is available on respective website [www.danskebank.fi](http://www.danskebank.fi).

When "Danske Bank" or "we" is used below it includes Danske Bank A/S, Danske Bank A/S, Finland Branch, Danske Invest Fund Management Ltd's and Danske Mortgage Bank Plc's processing of personal data where applicable.

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 guardians, authorized representatives, holders of a power of attorney and other private 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 process?

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

- personal details such as your name, social security number or other national ID number, citizenship, country of residence, and proof of identity such as a copy 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, costs, assets, debt, credit rating and insurance policies
- information about collateral, including market value, construction and building data, property data, technical and economic data about the housing company, energy data and environmental aspects. Information about property, housing company and energy data can be asked from authorities and commercial operators or external real estate agents.
- information about your education, profession
- information about your investment targets
- information about your family and household
- information about your activities, nature and extend of business
- information if you as our private customer also are an entrepreneur
- data on the environmental, social and governance (ESG) impact of your business where you are a sole trader

- details about the services and products we provide to you, including accounts, cards, loans, credits, etc.
- When you are applying for a loan, information about your current and previous loans. The information is received from other creditors through the enquiry system maintained by Suomen Asiakastieto Oy.
- transaction data
- how you use our services and products and your preferences in relation to 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, e.g. by using cookies and similar technology on our website
- information about 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, including video surveillance
- telephone conversations with you

We process other personal data as necessary to provide you with specific products or services or if we are required by law to do so.

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 inform us of any changes.

### 3. What we use your personal data for

We process data about you to provide the best advice and solutions, protect you against fraud and fulfil our agreements with you.

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 facilities
- digital banking solutions
- investment services and advice

We process personal data for the following purposes:

- For potential customers, to be able to offer you our products and services, and, if you choose to accept

one or more of our products or services and become a customer, for onboarding purposes in relation to identification and verification for anti-money laundering purposes.

- Customer services and customer relationship management, including advice, administration, credit assessment and verification of income data, credit control, recovery of outstanding debt, handling of complaints and to make information available to service providers authorised to request information about you.
- 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 using data analytics and statistics to improve products and services and to test our systems as well as to develop, train and test various models. We may also use anonymization for this purpose.
- Fraud detection and prevention including the processing of behavioural data to detect and prevent fraudulent activity in your accounts by identifying unusual, atypical or suspicious use, as well as registration of cards, such as Mastercards on relevant lists of blocked cards.
- To enable Danske Bank or third parties to pursue statistical, scientific and research purposes as part of research projects or similar, including anonymisation of personal data for such purposes.
- Marketing of our services and products, including marketing on behalf of other entities of the Danske Bank Group or our business partners, if we have your permission for this or are allowed such marketing by law. We use cookies and similar technology on our website and in our apps, including for marketing via digital channels and social media platforms. We refer to our cookie policy for further information.
- To comply with applicable laws and for other regulatory, administrative and compliance purposes, including identification, and verification of customers or their representatives according to anti-money laundering legislation, risk management, and prevention and detection and investigation of money laundering, terrorist financing, fraud and other types of financial crime. In relation to anti-money laundering and preventing of financing terrorism, identification and customers due diligence data is collected and verified at regular intervals during your customer relationship with us as required by law.
- To check, test and monitor our compliance with internal company policies and rules, regulatory and

legislative requirements, e.g. in relation to data protection, financial crime or market integrity.

- Security and crime prevention, including the use of video surveillance in 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 given us consent to use your personal data for a specific purpose, cf. the GDPR, art. 6.1(a)
- You have entered into or are considering entering into an agreement with us on a service or product, cf. the GDPR, art. 6.1(b)
- To comply with a legal obligation, cf. the GDPR, art. 6.1(c), for example, in accordance with
  - the Finnish Act on Detecting and Preventing Money Laundering and Terrorist Financing (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017)
  - the Finnish Tax Assessment Procedure Act (Laki verotusmenettelystä 1558/1995)
  - the Finnish Consumer Protection Act (Kuluttajansuojalaki 38/1978)
  - the Finnish Act on Strong Electronic Identification and Electronic Signatures (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009)
  - the Finnish Bookkeeping Act (Kirjanpitolaki 1336/1997)
  - the Finnish Credit Information Act (Luottotietolaki 527/2007)
  - the Finnish Act on Credit Institutions (Laki luottolaitostoiminnasta 610/2014)
  - the Finnish Payment Services Act (Maksupalvelulaki 290/2010)
  - the Finnish Act on Electronic Communications Services (Laki sähköisen viestinnän palveluista 917/2014)
  - General Data Protection Regulation (GDPR) and the Danish and Finnish Data Protection Act ((Tietosuojalaki 1050/2018)
  - the Finnish Securities Markets Act (Arvopaperimarkkinalaki 746/2012)
  - the EU Regulation on markets in financial instruments (MiFIR)
  - the EU Regulation on market abuse (the Market Abuse Regulation)

- the Finnish Act on Common Funds (Sijoitusrahastolaki 213/2019)
- The Finnish Act on Bank Account and Payment Account Monitoring System (Laki pankki- ja maksutilien valvontajärjestelmästä 571/2019)

- It is necessary to pursue a legitimate interest of Danske Bank, cf. the GDPR, art. 6.1(f). For example, this may be for documentation and security purposes, to prevent and detect money laundering, to prevent and detect fraud, abuse and loss, to strengthen IT and payment security and for direct marketing purposes. We will do so only if our legitimate interest in each case is not outweighed by your interests or rights and freedoms.

#### 5. Sensitive personal data

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

##### Types of sensitive personal data

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

- Trade union membership information
- Biometric data, for example via facial recognition technology
- Information about your religious or philosophical beliefs
- Information about your political opinions

We also process sensitive personal data that may appear in the information you give us and transactions you ask us to execute.

##### Purposes for processing sensitive personal data

We will process sensitive personal data only when we need to, including

- for the purpose of a product or service we provide to you
- for the purpose of giving you discounts related, for example, to trade union membership
- for identification and verification purposes
- for the prevention and detection of money laundering and other types of crime, including for fraud prevention and detection purposes
- to comply with legal requirements that apply to us as a financial institution

##### Legal basis for processing sensitive personal data

We may process sensitive personal data about you on the legal basis of

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

## 6. How do we collect the information we have about you?

### Personal data collected from you

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

- fill in applications and other forms for ordering services and products
- submit specific documents to us
- participate in meetings with us, for example with your adviser
- talk to us on the phone
- use our website, mobile applications, products and services
- participate in our customer surveys or promotions organised by us
- communicate with us via letter and digital means, including e-mails, or social media

### Electronic communication recording and monitoring, including voice recordings

We are obliged to record and store all electronic communications related to investment services, for instance when we chat, email or speak on the phone with you. We store this information for as long as we are legally required to.

Incoming and outgoing calls may be recorded, listened to and stored for compliance with regulatory requirements but also for documentation purposes.

### Cookies

We use cookies and similar technology on our websites and in our digital apps. When you first enter one of our websites or download our apps, we set cookies that are needed to enable you to use our services (necessary cookies). If you consent to additional cookies, such as functional, statistical and/or marketing cookies, we will set cookies according to your choice to measure, analyse and improve the use and performance of our products and services and to send you relevant marketing messages.

Some of the marketing cookies are owned by third parties, e.g. Google. We continue to be responsible for third party use of your data which is processed for our benefit (shared data controller responsibility). We refer to our [cookie policy](#) for further information.

### Personal data collected from third parties

We receive and collect data from third parties, including from

- Shops, banks, payment and service 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.
- Members of your household if they are customers, in order to perform required disposable income calculations.
- If you have a joint account with someone, we may collect information about you and your joint account from your co-account holder.
- Digital and Population Data Services Agency (Digi- ja väestötietovirasto) the Finnish Trade Register (Kaupparekisteri), the Finnish Real Property Register (Kiinteistörekisteri) and other publicly accessible sources and registers as well as the Finnish Trust Network. Sometimes we collect this data via other service providers that provide the data. We process the data, for example for identification and verification purposes and to check data accuracy.
- The National Land Survey of Finland and house managing agencies, Central Federation of Finnish Real Estate Agencies, external house inspectors, Energy certificate registry, Fellowmind Finland Oy Ab, insurance companies and real estate agencies for collection of information regarding collateral.
- Credit rating agencies and warning registers, including Suomen Asiakastieto Oy. We process the data to perform credit assessments as well as to fulfil our legal obligation to know our customers. We update the data regularly.
- Other entities of the Danske Bank Group if we have your consent or if it is allowed under law, for example to provide you with better customised products and services.
- Other entities of the Danske Bank Group if existing legislation allows or requires us to share the information, for example if it is necessary to comply with group-based management, control and/or reporting requirements established by law, or the sharing of notifications to Finnish Financial Intelligence Unit (Rahanpesun selvittelykeskus) in accordance with anti-money laundering legislation .

- External data processors, business partners (including correspondent banks and other banks) and vendors 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 or to prevent the circumvention of sanctions.

#### 7. Third parties that we share your personal data with

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

- Other entities of the Danske Bank Group if we have your consent or if it is allowed under law, for example to provide you with better customised products and services.
- Other entities of the Danske Bank Group if existing legislation allows or requires us to share the information, for example if it is necessary to comply with group-based management, control and/or reporting requirements established by law, or the sharing of notifications to the Finnish Financial Intelligence Unit (Rahanpesun selvittelykeskus) in accordance with anti-money laundering legislation.
- 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 authorised 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.
- Card issuers, payees and holders of lists of blocked cards, e.g. Nets, in case you request us to block your debit or credit card or if we have reasonable suspicion of card abuse.
- Other creditors via enquiry system maintained by Suomen Asiakastieto Oy, where we can disclose information about your loans with your consent and according to your order.
- Guarantors, including the Social Insurance Institution of Finland (Kela), State Treasury (Valtiokonttori), Finnish P&C Insurance Ltd (Suomen Vahinkovakuutus Oy), Garantia Insurance Company Ltd (Vakuutusosakeyhtiö Garantia), Guarantee Foundation (Takuusäätiö), pledgers, individuals holding a power of attorney, lawyers, accountants or others you have authorised us to share the information with.
- If you have joint financial products with someone, such as joint account, we may share your information with your co-product holder/owner.
- External data processors, business partners (including correspondent banks and other banks) and vendors 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 or to prevent and detect money laundering, fraud, abuse and loss.
- Our suppliers, including lawyers, accountants, consultants and courier services. We use courier services to deliver, for example, credit cards to you, and we disclose your name, address and telephone number to them, so you can receive the consignment.
- Data processors, including other units of the Danske Bank Group and IT service providers who may be located outside the EU and the EEA.
- Social media companies.
- 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 Finnish Financial Intelligence Unit in accordance with the Finnish Anti-Money Laundering Act, the Finnish tax authorities in accordance with the Finnish Tax Proceedings Act, the register of bank and payment accounts maintained by the customs and the Bank of Finland for statistical and other purposes.
- Regulators, such as the Danish and the Finnish Financial Supervisory Authority (DK:Finanstilsynet, FI: Finanssivalvonta), law enforcement agencies and authorities in Finland and other countries, including countries 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 social and economic research or statistics purposes, where it is in the public interest.

## 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 in Australia, Canada and India.

When Danske Bank transfers 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 safeguarding by

- ensuring that there is an adequacy decision by the European Commission
- using standard contracts approved by the European Commission or the Danish Data Protection Agency

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, evaluate the likelihood of default risk and value assets and for marketing purposes. If you are a sole trader, we use profiling and data modelling to assess the environmental, social and governance (ESG) risk of your business.

### Automated decision-making

With automated decision-making, we use our systems to make decisions without any human involvement on the basis of 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 and 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 determine the amount we can lend you. The information used in the assessment may come from you or the customer information we have stored about you on the basis of the customer relationship, or from third parties, such as credit information registers. We evaluate the application and other information and make a decision based on our own lending criteria. Your application may be disapproved if, for example, we determine that you are insolvent or have payment defaults.

In relation to the prevention and detection of money laundering, we perform identity and address checks against public registers and sanctions checks.

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 executing 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. "Your rights" and "Rights related to automated decision-making".

## 10. For how long do we store your personal data?

We keep your data only for as long as it is needed for the purposes for which your data was registered and used. The data will subsequently be deleted or irreversibly anonymised.

When your business relations with us have terminated, we normally keep your data for another seven years. This is due primarily to our obligations under the Finnish Bookkeeping Act, the Finnish Anti-Money Laundering Act and requirements from the Danish and Finnish Financial Supervisory Authority. In certain circumstances, we keep your information for a longer period of time. This is the case, for example,

- if the limitation period is 10 years with the addition of an administrative case management buffer should a

claim or matter arise at the end of the applicable limitation period or if retention is required due to other regulatory requirements.

If you, as a potential customer, have asked for an offer for a loan or another product or service, but refuse the offer and do not become a customer, your personal data will normally be stored for six months, but may for some purposes be stored longer to comply with other legal obligations, for example due to regulatory requirements.

### 11. Your rights

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

- contact us on our main telephone number (+358 200 2580 )contact your adviser directly if you have one

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

#### Right to access your personal data

You may request access to the personal data we process and information about where it comes from and what we use it for. You can obtain information about the period for which we store your data and about who receives data about you, to the extent that we disclose data in Finland and abroad. Your right of access may, however, be restricted by legislation, protection of other persons' privacy and consideration for our business and practices. Access to video surveillance may be restricted due to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to employees. Our know-how, business secrets as well as internal assessments and material may also be exempt from the right of access.

Under the "Profile" section of the Danske Mobile Banking app, you can get an overview of certain data we are processing about you. You will for example find your contact details and information you have given us about your household, income and debt. You can update the information if changes have occurred in your life.

If you wish to exercise your right of access under GDPR, please write to [GDPR-insight@danskebank-fi](mailto:GDPR-insight@danskebank-fi).

#### 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 object to the decision, and you can request a manual review of any automated decision.

#### Right to object

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

#### 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 have the data rectified. If data is incomplete, you are entitled to have the data completed, including by means of providing us with 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 it was collected.

However, in the following cases, we may or are required to keep your data:

- For compliance with a legal obligation, for instance if we are obliged by law to hold your data for a certain period of time, for example according to Finnish anti-money laundering legislation or the Finnish 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 defense 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 the data to storage. Use will be restricted to storage only until the correctness of the data can be verified, or it can be checked whether our legitimate interests outweigh your interests.

If you are entitled to have the data we have about you erased, you may instead request us to restrict the use of the data to storage. If we need to use the data solely to assert a legal claim, you may also demand that other use of the data be restricted to storage. We may, however, be entitled to use the data for other purposes, for instance 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 may withdraw your consent at any time with future effect. Please note that if you withdraw your consent, we may not be able to offer you specific services or products. Note also that we will continue to use your personal data, for example to fulfil an agreement we have made with you or if we are required by law to do so.

#### **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 a copy of the data you have provided in a digital machine-readable format.

### **12. Changes to this privacy notice**

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

### **13. Contact details and how to 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 on our main telephone number (+358 200 2580). You are also welcome to contact your adviser directly.

You can contact our Data Protection Officer by email at [dpofunction@danskebank.com](mailto:dpofunction@danskebank.com).

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 by contacting directly our customer service or branches, via eBanking message or by filing your complaint on [www.danskebank.fi/sinulle/asiakaspalvelu/anna-palautetta/reklamaatit](http://www.danskebank.fi/sinulle/asiakaspalvelu/anna-palautetta/reklamaatit). You can also lodge a complaint with the Data Protection Agency: Tietosuojavaltuutettu, Lintulahdenkuja 4, 00530 Helsinki, email: [tietosuoja@om.fi](mailto:tietosuoja@om.fi).

If, for example, your residence or the place of the alleged infringement is in or is related to another member state than Finland, you can typically also lodge a complaint with the supervisory authority for data protection in that member state.