Privacy notice for personal customers and other private individuals

Effective from 26 March 2025

1. Our role as data controller and the reason for this privacy notice

This privacy notice applies to the processing of personal data related to personal customers, retail customers, sole traders and other private individuals by Danske Bank A/S, Finland Branch (Danske Bank) as data controller. 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, Finland Branch
Business ID 1078693-2
Televisiokatu 1, 00075 DANSKE BANK (Finnish branch of Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark, (CVR 61126228))

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

"Danske Bank" or "we" below refers to the processing of personal data by Danske Bank A/S, Danske Bank A/S, Finland Branch, Danske Invest Fund Management Ltd and Danske Mortgage Bank Plc as applicable.

The Bank has appointed a Data Protection Officer (DPO), whose contact details are as follows:

DPO of Danske Bank A/S,
Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark
Email address: dpofunction@danskebank.dk

We process information about you (personal data), and this privacy notice applies to personal customers, retail customers as well as privately owned businesses (sole traders) and other private individuals, such as guarantors, pledgers and, where applicable, to other individuals connected to a customer such as guardians, authorised representatives, holders of powers of attorney and other private individuals with whom Danske Bank interacts and collaborates.

This privacy notice sets out how and why and on what legal basis Danske Bank processes your personal data and how we protect your privacy rights.

See section 12 for more information on how to contact Danske Bank in case you have questions related to how Danske Bank processes your personal data.

2. Types of personal data we collect and process

Depending on the services and products you have or are interested in and the necessity of processing personal data in that respect, we collect and process various types of personal data, including, but not limited to, the examples of personal data listed below:

- Identification information, 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 license and/or birth certificate
- Contact information, including your address, telephone number and email address

- Financial information, including information about your income, assets, debts, credit ratings, insurances, pensions, taxes, environmental impact, life situation and members of your household (number and age of persons)
- Information on security and collateral, including market values, 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.
- Registration number of the object of financing
- Educational information, such as your education, occupation
- Environmental information and data on the social and governance (ESG) impact of your business (if you own a private business)
- Information about the services and products we provide to you, including information about accounts, cards, loans, credits, etc.
- Information on how you use our services and products and your preferences in relation to them
- Information about your current and previous credits and income or benefits for the assessment of your creditworthiness. The information is received from other creditors through the enquiry system maintained by Suomen Asiakastieto Oy or from the Positive Credit Register maintained by the Incomes Register unit of the Finnish Tax Administration.
- Personal credit information from the credit information register for the assessment of creditworthiness or for other purposes based on law
- Transaction data
- Information related to your use of our websites, platforms and digital applications, including - to the extent applicable and necessary - traffic, location, tracking and communication data, e.g. collected by use of cookies and similar technology, cf. also Cookie policy
- Tracking data if you have consented to this in connection with signing up for receiving newsletters
- Information about your devices used to access our websites as well as technical information, including the type of device and operative systems
- Information about you and your preferences provided by you in connection with various types of marketing and events
- Video recordings when you visit our premises
- Recordings of phone conversations and online meetings with you, cf. Recording of phone conversations and online meetings
- Transcriptions and summaries of discussions held with you during online meetings, cf. Automatic transcription and summary of online meetings using AI technology
- 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 possible advice and solutions for you very much depends on how well we know you and, consequently, it is important that the information you provide is correct and accurate and that you inform us of any changes.

3. Why & on which legal basis we process your personal information

Generally, we process personal information about you to provide you with the services and products you have chosen, to offer you the best advice and solutions, to protect you and Danske Bank against fraud, to fulfil our agreements with you and to comply with applicable regulations, including data security and data protection requirements.

Below, we list some examples of why and on which legal basis we process your personal data in various contexts:

- When we onboard you as a customer, we process your personal data for identification, verification and anti-money laundering purposes. The legal basis for this processing is to comply with a legal obligation*, cf. GDPR art. 6.1(c), for example, pursuant to the Finnish Act on Preventing Money Laundering and Terrorist Financing (Laki rahanpesun ja terrorismin rahoittamisen estämisestä).
- When we provide you with the financial product you have requested or consider obtaining (such as payment services, accounts, card services, loans, credit facilities, digital banking solutions, investment services and financial advice) we process your personal data because you have entered into or are considering entering into an agreement with us on a service or product, cf. GDPR art. 6.1(b) and to pursue legitimate interests, cf. GDPR art. 6.1(f). Such processing may include for example: customer services, customer relationship management, including registration in our CRM systems,

administration, credit assessment and verification of income data, credit control, recovery of outstanding debt, handling of complaints and/or making information available to service providers authorised to request information about you.

- If, for instance, transfer your personal data to a third party for budget building or if we propose to transfer your personal data to a partner so you may receive a quotation for a product or a service, we may do this because you have given us consent to using and sharing your personal data for such specific purposes, or you have requested the service cf. GDPR art 6. (b).
- When we communicate with you about the products and services you have requested or send you information on our system updates, we do so to fulfil a contract with you, cf. GDPR art. 6.1, (b), or subject to a legal obligation*, cf. GDPR art. 6.1(c), or to pursue a legitimate interest, cf. GDPR art. 6.1(f).
- When we improve, develop and manage our IT-systems, we may use your personal data for analytics to improve or develop products and services and test our systems or to develop, train and test IT-models. This may be done on the legal basis we have for processing your personal data in our IT systems in the first stage of processing (which could be any of the legal bases mentioned in this section), and/or to ensure a sufficient level of security, cf. GDPR art. 6.1(c), or we may pursue a legitimate interest, cf. GDPR, art. 6.1(f).
- When we set fees and prices for our products and services, including using data analytics and statistics for such purpose, we do this to fulfil contractual purposes, cf. GDPR art. 6.1 (b), so that you may receive a price quotation or similar.
- When we carry out fraud detection on card and account transactions, including processing of behavioral data to detect and prevent fraudulent activity in our accounts by identifying unusual, atypical, or suspicious use, as well as registration of payment cards on relevant lists of blocked cards, as well as detection and prevention of fraud, credit fraud and other types of financial crimes, we do so to comply with legal obligations*, cf. GDPR art. 6.1(c), and to pursue legitimate interests, cf. GDPR art. 6.1(f).
- When we pursue statistical, scientific and/or research purposes as part of research projects or similar, including anonymization of personal data for such purposes, we pursue legitimate interests, cf. GDPR art. 6.1(f) or we act in the public interest of, cf. GDPR art. 6.1 (e).
- When we carry out profiling and marketing of our services and products, including marketing on behalf of other legal entities of the Danske Bank Group, we do so if we have your consent to this, cf. GDPR art. 6.1(a), or we pursue legitimate interests, cf. GDPR art. 6.1 (f).
- We use cookies and similar technology on our website and in our apps for functional, statistical and marketing purposes via digital channels and social media platforms if you have consented to this, cf. the cookie requirements for collection of data and GDPR, art. 6.1(a) for the subsequent use of data. We refer to our cookie policy for further information (Cookie policy).
- When we assess, 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, we process your personal data subject to legal obligations*, cf. GDPR art. 6.1(c) and to pursue legitimate interests of Danske Bank, cf. GDPR art. 6.1(f).
- We process your personal data for security reasons, for instance various loggings, cf. GDPR art. 6.1(c) and art. 32.
- We use video surveillance and record in our branches and other premises, reception and customer areas where we are pursuing legitimate interests, cf. GDPR art. 6.1(f).
- When we collect, share and use personal data to build, maintain and use models for credit risk exposure and Internal Ratings Based (IRB) modelling to assess capital requirements, we do so with reference to the Capital Requirement Regulation (CRR) which is required as part of the bank's risk management, cf. GDPR art. 6.1(c).
- When we send you newsletters, we process your personal data, and we use your email and name for documentation purposes to send you articles, news and updates because you have requested this service from us, cf. GDPR art. 6.1(b) and based on your consent, cf. GDPR art 6.1 (a). We may also invite you to events and send you marketing material in areas that we think may have your interest, and we track which articles have your interest and which you open based on your consent, cf. GDPR art. 6.1(a).
- We also carry out several other legal, regulatory, administrative and compliance-related processing activities which entail processing of personal data, including identification and verification according to anti-money laundering legislation, sanction lists, risk management, and detection and prevention of fraud, credit fraud and other types of financial crimes, all based on legal obligations*, cf. GDPR art. 6.1(c).

* When we refer to processing of your personal data due to 'legal obligations', this refers to qualifying legal requirements in any of the following legislations (please note that this list is not exhaustive):

- The Finnish Act on Preventing Money Laundering and Terrorist Financing (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017)
- Various Finnish tax acts, including the Tax Assessment Procedure Act (Laki verotusmenettelystä 1558/1995)
- The Finnish Accounting 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 Bank Account and Payment Account Monitoring System (Laki pankki- ja maksutilien valvontajärjestelmästä 571/2019)
- The Finnish Act on Positive Credit Information Register (Laki positiivisesta luottotietorekisteristä 739/2022)
- The Finnish Act on Electronic Communications Services (Laki sähköisen viestinnän palveluista 917/2014)
- The Finnish Securities Markets Act (Arvopaperimarkkinalaki 746/2012)
- The Finnish Act on Common Funds (Sijoitusrahastolaki 213/2019)
- The Finnish Act on Strong Electronic Identification and Electronic Signatures (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009)
- The Finnish Consumer Protection act (Kuluttajansuojalaki 38/1978)
- The EU Regulation on Market Abuse (the Market Abuse Regulation, Markkinoiden väärinkäyttöasetus 596/2014)
- The EU Capital Requirement Regulation (CRR) (Asetus luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvaatimuksista 575/2013)
- The Finnish Debt Collection Act (Laki saatavien perinnästä 513/1999)
- The EU Markets in Financial Instruments Regulations (MiFID I and II)
- The General Data Protection Regulation (GDPR) (Yleinen tietosuoja-asetus 2016/679)
- The Finnish Data Protection Act (Tietosuojalaki 1050/2018)

4. Sensitive personal data

Some of the information we process about you may be sensitive personal data (also known as special categories of data). Sensitive personal data may e.g., be information about your health or information about your membership of a trade union.

Sensitive personal data is subject to specific processing conditions, and we try to avoid processing such personal data when possible. However, in some instances we need to process sensitive personal data about you.

Below you can see examples of types of sensitive personal data we process about you, why we do it and our legal basis (exceptions in GDPR art. 9) for doing so:

- For certain products or services, we may ask to process your sensitive personal data for the purpose of providing you with benefits relating to your Trade Union membership with your consent, cf. GDPR, art. 6.1(a) and 9.2(a).
- We may process sensitive personal data about you to comply with legal requirements that apply to us as a financial institution with legal basis in other legislation, cf. GDPR art. 6.1(c), 9.1 (g) and 9.3.
- We may process sensitive personal data about you if such processing is necessary for the establishment, exercise or defence of legal claims, cf. GDPR art. 9.1(f).

5. How we collect the personal data we have about you

Personal data collected from you

We collect information that you share with us or that we obtain by observing your actions, including for example when

- 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, either on our premises or in an online meeting
- Talk to us on the phone
- Use our website, mobile applications, products, and services
- Participate in our customer surveys or promotions organized by us
- Communicate with us by letter and digital means, including emails, or on social media
- Use our digital solutions and Apps or visit our websites
- Provide us with your household information
- We collect personal data from electronic communications, telephone and video recordings
- Tracking on your subscription to newsletters

We are obliged to monitor and store all electronic communications related to investment services, for instance when we chat, email or speak on the phone with you. We also store video recordings of you if you have visited our premises.

Incoming and outgoing calls and online meetings are recorded, listened to and stored to comply with regulatory requirements but also for documentation purposes. We refer to our information on recording of phone conversations for details on our recording and processing of personal data in relation to voice and online meeting recordings (Recording of phone conversations and online meetings).

Personal data collected from use of cookies

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

Some of the marketing cookies are owned by third parties. We share responsibility (joint controllership) for such third parties' use of your personal data which is collected by use of cookies and processed for our benefit. We refer to our cookie policy (Cookie policy) for further information.

Personal data we collect from third parties

We receive and collect personal data from third parties, including for example from:

- Shops, banks, payment and service providers when you use your credit or payment cards or other payment services. We process the personal data to execute payments and prepare account statements, payment summaries and the like.
- Members of your household if they are customers, to perform required disposable income calculations.
- If you have a joint account with someone, we collect information about you from your co-account holder.
- Digital and Population Data Services Agency (Digi- ja väestötietovirasto), the Finnish Trade Register (Kaupparekisteri), 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., cf. GDPR art. 6.1(f), section 29 of the Finnish Data Protection Act and Chapter 15 Section 18 in the Finnish Act on Credit Institutions.

- The National Land Survey of Finland, house managing agencies, Central Federation of Finnish Real Estate Agencies, external house inspectors, Energy certificate registry, Fellowmind Finland Oy Ab, Alma Media Oyj, insurance companies and real estate agencies (for collection of information regarding collateral).
- Suomen Asiakastieto Oy as a company engaging in credit reference services. We process the data to perform credit assessments and to comply with our legal obligation to know our customers in accordance with anti-money laundering legislation. We update the data regularly. The Positive credit register maintained by the Incomes Register unit of the Finnish Tax Administration. We process data for the assessment of creditworthiness, for credit control and for other lawful purposes.
- Guarantors
- Other entities of the Danske Bank Group, if we have your consent, for example in order to provide you with better customized 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, such as the Capital Requirement Regulation (CRR).
- External data controllers, such as cooperation partners/ business partners (including correspondent banks and other banks) and vendors, if we have your consent or if permitted under existing legislation, for example in order 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.

6. Third parties that we share your personal data with

We will keep your information confidential under applicable banking secrecy rules. However, where we have due cause as per some of the examples set out below, we may disclose and share relevant personal data with group companies and third parties, who are also obliged to keep your personal data confidential:

- Other entities of the Danske Bank Group, for example to provide you with better customized 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 or risk management requirements imposed by law or regulations (e.g. Capital Requirement Regulation) and/or reporting requirements established by law or required by regulators.
- Finnish Financial Intelligence Unit (Rahanpesun selvittelykeskus) in accordance with anti-money laundering legislation.
- If you have asked us to transfer money to others, we disclose personal data about you that is necessary to identify you and to perform the transaction.
- When we process your international payments, your personal data may be processed by Swift in the context of the Swift's Transaction Processing Services, which enable us to send and receive financial messages or files, and to pre-validate, track and manage financial transactions.
- Euroclear Finland Ltd for settlement of trades
- Service providers 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.
- Card producers, when cards are imprinted with your personal data.
- 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 or for Nets to be able to prevent fraud.
- 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.
- The Positive credit register maintained by the Incomes Register Unit of the Finnish Tax Administration. We report the information about your credits, collateral and arrears as required by law to the Positive credit register.
- 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 authorized us to share information with.

- If you have joint financial products with someone, such as a joint account or a child savings account, we share your information, including personal identification number, with your co-product holder/owner and for tax reporting purposes.
- Nets, other banks and EBA Clearing, if required or permitted under existing legislation, to prevent and detect money laundering, fraud, card abuse and loss.
- Lawyers, accountants, consultants.
- 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.
- IT service and outsourcing providers as well as personal data processors to provide services to us and you.
- External data controllers, such as cooperation partners/ business partners (including correspondent banks and other banks) and vendors, if we have your consent or if permitted under existing legislation, for example in order 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.
- Social media companies when you have given your consent for direct marketing purposes
- 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 (Rahanpesun selvittelykeskus) in accordance with the Finnish Act on Preventing Money Laundering and Terrorist Financing, the Finnish tax authorities in accordance with the Finnish Tax Proceedings Act, the Bank and Payment Accounts Register maintained by the Finnish Customs and the Bank of Finland for statistical and other purposes.
- Regulators, such as the Danish and Finnish Financial Supervisory Authority (DK: Finanstilsynet, FI: Finanssivalvonta), the Danish and Finnish Data Protection Authorities (DK: Datatilsynet, FI: Tietosuojavaltuutetun toimisto), law enforcement agencies and authorities in Finland or abroad in connection with their duties.
- Credit reference agencies. If you default on your obligations to Danske Bank, we may report you to credit reference agencies in accordance with applicable law.
- Debt collection agencies. If you default on your performance on a credit agreement, we will transfer information of your debt to a debt collection agency.
- For social and economic research or statistics purposes, including where it would be in the public interest.
- In connection with transactions (including transfers, asset sales, mergers and acquisitions) which entail transfer of all or part of your business to another company, we may share your personal data to the extent necessary to complete the transfer and your customer relationship within the framework of the legal requirements we have to comply with.

7. Profiling and automated decisions

Profiling

We are constantly working to develop, improve and manage our products and systems. We use data analysis and statistics and evaluate our analyses, models and theories on customer behaviour with the use of advanced analytical innovative methods, such as machine learning and AI. This helps us, for example, to set fees and prices and provides the basis for our marketing and business development. We continually process customer personal data, develop profiles with the use of machine learning models to help us to offer products that meet our customer's unique needs and prioritise customer enquiries in an efficient way. We also process personal data for process and system development and improvement purposes, including through tests.

We use transactional, behavioural and demographic personal data for statistical analysis and for developing new models, products and services. We analyse both publicly available data, internal data, including data from other Group Companies, and external data. The analyses allow us to create customer profiles and capture life-changing events, such as first job, home purchase or retirement. We do this to be a relevant bank for our customers and to provide the best financial advice. Our

processing of personal data for the abovementioned purposes is always based on an appropriate legal basis, such as your consent, and you will be informed in more detail when we use your personal data in such a process.

We use cookies and similar technology on our websites and in our digital apps for marketing purposes, including for marketing via digital channels and social platforms such as Facebook. You can read more about this in our Cookie policy.

Automated decision-making

With automated decision-making, we use our systems to make decisions without any human involvement based on the personal data we have about you. Depending on the specific decision, we also use personal information from public registers and other public sources. Automated decision-making helps us ensure that our decisions are quicker and more fair, efficient and correct as compared to a similar manual process.

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.

We will always inform you directly when we use your personal data in a process with automated decision making.

An example of our use of automated decision-making processes is in relation to loans and credit cards, where we use 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 of money we can lend you.

See section, 10 'Your rights', for information on your rights in relation to automated decisions.

8. Transfer of personal data to third countries

Your personal data may be processed by our business partners within the EU/EEA in connection with our request to provide you with various services on our behalf.

In some cases, we use various IT-suppliers, business partners and consultants, etc., who can access personal data from countries outside the EU/EEA ("third countries"), if necessary, despite such personal data generally not being stored in these third countries. Such IT-providers, partners, etc. are subject to data processing or data sharing agreements with us, which ensure that they process personal data only in accordance with the GDPR and applicable EU and national data protection laws.

We primarily choose providers/partners that process personal data within the EU/EEA, and secondly suppliers in countries that appear on the EU Commission's list of safe third countries, and only, if necessary, suppliers in other third countries. Accordingly, we rely on different legal bases depending on the country of the personal data recipient:

- If we transfer your personal data to parties in countries where the European Commission has found that the country ensures an adequate level of protection, we rely on the adequacy decision of the European Commission as our GDPR art. 45 transfer basis.
- If we transfer your personal data to parties located in the USA, we may rely on the EU-US Data Privacy Framework to certified parties as our GDPR art. 45 transfer basis.
- If we transfer your personal data to other third countries, we may rely on the European Commission's standard contractual clauses (also known as SCCs) or business partner's binding corporate rules (also known as BCRs) together with implementation of adequate supplementary measures or carry out a review of local legislation to ensure that your personal data receives an essentially equivalent level of protection to that guaranteed in the EU/EEA, if and where deemed necessary as our legal basis for transfer under GDPR art. 46.

- We may also 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 defense of a legal claim.

When transferring personal data to a business partner outside of the EU/EEA, we ensure that our transfer of your personal data is conducted in accordance with GDPR Chapter V.

You can read more on personal data transfers to third countries:

- on the website of Data Protection Ombudsman's Office: Transfers of personal data out of the European Economic Area - Data Protection Ombudsman's Office and
- on the EU Commission's website: Rules on international data transfers - European Commission

9. How long do we store your personal data?

We keep your personal data only for as long as it is needed for the specified purposes for which your personal data was registered and used or as required by law for the purpose. The personal data will subsequently be deleted or irreversibly anonymized.

We have many different processes where we use your personal data and many different legal bases for retention of your personal data. Our retention criteria and retention periods vary from a few minutes up to 30 years. Below you see some examples of retention periods, but please note that the list is not exhaustive:

- We keep your Know Your Customer information for as long as you are a customer and for an additional 5 years as required by the Finnish Act on Prevention of Money Laundering and Terrorist Financing.
- We keep your consent to our use of cookies for one year unless you withdraw it earlier.
- We keep your voice recordings for 5 years for general documentation purposes, and if the voice recording relates to investments, we have a legal obligation to keep it for 7 years under MiFID II.
- If you, as a potential customer, have asked for an offer for a loan or another product or service, but decline 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 under the Finnish Act on Prevention Money Laundering and Terrorist Financing

10. Your rights

Your rights in relation to personal data are described below. To exercise your rights, you can use any channel to contact us, for example:

- Contact us on our main telephone number (+358 200 2580).
- Contact your adviser directly, if you have one, or via message in Danske eBanking or Danske Mobile Banking.

See section 12 for more information on how to contact Danske Bank about data protection.

Right to access your personal data

You have the right to request access to your personal data and to request information about the processing we carry out. 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.

If you wish to exercise your right of access under the GDPR, the best way to contact us is to make an order at: Order a personal data overview, or alternatively write to GDPR-insight@danskebank.fi. However, you may also contact us via your adviser or via message in Danske eBanking or Danske Mobile Banking.

In the Profile section of Mobile Banking, you can also get an overview of the most common data we process about you, and you can update the information if there have been changes.

Rights related to automated decision-making

When we use automated decision-making in our processes, you will always be notified separately in advance about our legal basis for this and your option to not to be subject to the automated decision making. Furthermore, you will be informed about the reasoning behind the automated decision-making, and you will be given the opportunity to express your point of view, and to object to the decision, and of your right to request a manual review of any automated decision.

Right to object to processing

In certain circumstances, you have the right to object to the processing of your personal data, for instance when we use automated decisioning-making processes, or, for example, when the processing is based on our legitimate interests.

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

Right to rectification of your data

If your personal data is inaccurate, you are entitled to have your personal data rectified. If your personal data is incomplete, you are entitled to have the personal 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 personal data erased if the personal data is no longer necessary for the purposes for which it was collected. However, in the following cases, we are required to keep your personal data:

- To comply with a legal obligation, for instance if we are obliged by law to hold your personal data for a certain period, for example according to the Finnish Act on Prevention on Money Laundering and Terrorist Financing or the Finnish Accounting Act. In such situations, we cannot erase your personal data until the required retention period has expired.
- For the performance of a task carried out in the public interest, such as sending statistical data to the Bank of Finland (Suomen Pankki).
- For establishment, exercise, or defense of legal claims.

Restriction of use

If you believe that the data that we have registered about you is incorrect, or if you have objected to our use of the data, you are entitled to obtain restricted processing of your personal data for storage only until we can verify the correctness of the data or if our legitimate interests outweigh your interests or not.

Withdrawal of a consent

Where consent is the legal basis for a specific processing activity, you can always withdraw your consent at any time by contacting the bank (see the section above or section 12). Please note that if you withdraw your consent, we may not be able to offer you specific services or products. Please also note that we will continue to use your previously collected personal data, for example in order to fulfil an agreement we have made with you or if we are required by law to do so. Some consents are provided for one action only (such as consent to sharing personal data with a third party), also called one-time consents. Withdrawal of a one-time consent will not have legal effect due to the nature of the consent.

Data portability

You have the right to receive personal data which you have provided to us yourself in a structured, commonly used and machine-readable format for personal use. You also have the right to request that we transmit this data directly to another data controller.

11. Changes to this privacy notice

We are required to update this privacy notice on a regular basis. When we do, you will see that the 'effective from' date at the top of this document changes. 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).

12. 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) or contact your adviser directly, if you have one, or via message in Danske eBanking or Danske Mobile Banking, or you can send us a letter to Danske Bank A/S, Finland Branch, Televisiokatu 1, 00075 Danske Bank, Finland.

You can contact our data protection officer with all questions on our use of your personal data by email to dpofunction@danskebank.com or by sending a letter to the above address.

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 also lodge a complaint with Finnish Office of the Data Protection Ombudsman: Tietosuojavaltuutettu, Lintulahdenkuja 4, 00530 Helsinki, email: tietosuoja@om.fi or the Danish Data Protection Authority: Datatilsynet, Carl Jacobsens Vej 35, DK- 2500 Valby, email address: dt@datatilsynet.dk .

If, for example, your residence or the place of the alleged infringement is in or is related to another member state than Finland or Denmark, you can typically also lodge a complaint with the data protection authority in that member state. You always have the option to try your case in court.