Danske Bank A/S, Danmark, Sverige Filial´s and Danske Hypotek AB's privacy notice for all individuals

Effective from 14 January 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, potential personal customers, sole trader customers, guarantors, pledgers and where applicable other individuals connected to a personal or corporate customer such as guardians, authorized representatives, holders of a power of attorney, employees or owners of a corporate customer and other individuals with whom we, Danske Bank A/S, Danmark, Sverige Filial, the Swedish branch of Danske Bank A/S, interact and collaborate with.

This Privacy Notice is also applicable on Danske Hypotek AB´s processing of personal data. Danske Hypotek AB is a wholly owned subsidiary of Danske Bank A/S.

Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark, CVR 61126228, with the Swedish branch Danske Bank A/S, Danmark Sverige Filial, reg.no 516401-981, Box 7523, 103 92 Stockholm, is the data controller for all processing of personal data described in this privacy notice except when administrating mortgage loans on behalf of Danske Hypotek AB. Danske Hypotek AB, Box 7523, 10392, Stockholm, Sweden, reg.no. 559001-4515, is in that situation the data controller and Danske Bank A/S is the processor.

When "Danske Bank" or "we" is used below it includes both Danske Bank A/S, the Swedish branch´s and Danske Hypotek AB´s processing of personal data where applicable.

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.

Please 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, personal identity number, coordination number or other national ID number, citizenship, country of residence, tax residence, tax registration number and proof of identity, such as a copy of your passport, driver's license and/or population registration certificate.
- contact information, including your address, telephone number and email address
- financial information, including information about your income, expenses, assets, debts, credit ratings, insurances, pensions, taxes and members of your household (number and age of persons)
- information on security and collateral, including market values, energy data and environmental aspects,
- information about your investment targets,
- information if you as our personal customer also is an entrepreneur,
- transaction data,
- educational information, such as your education, profession, work knowledge and experience
- environmental information and data on the social and governance (ESG) impact of your business (if you are a sole trader)
- information about the services and products we provide to you, including information about accounts, cards, loans, credits, pensions, etc.
- information on how you use our services and products and your preferences in relation to these

- 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 Danske Bank's cookie policy
- tracking data 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 and use Bankomat AB´s cash machines
- recordings of telephone conversations and of online meetings with you, , cf. Recording of calls and online meetings,
- 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 Swedish Anti-Money Laundering Act (lag (2017: 630) om åtgärder mot penningtvätt och finansiering av terrorism).
- 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, financial advice, insurance and pension services (in some cases by other companies in the Danske Bank Group), customer services, customer relationship management including registration in our CRM systems, administration, credit assessment, recovery of outstanding debt, handling of complaints and/or making information available to service providers authorised to request information about you), we do this 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).
- Sometimes we share or transfer your personal data to a third party because you have requested us to do so, so you could receive a quotation for a product or a service from our business partner, we may do this to fulfil an agreement with you cf. GDPR art. 6.1(b) to pursue legitimate interests, cf. GDPR art. 6.1(f) or you may have given us consent to use and share your personal data for such specific purposes yourself, cf. GDPR art. 6.1(a).
- When we communicate with you about the products and services you have requested or send you information on 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).
- During our constant efforts to improve the development, management and testing of our IT systems and products we use personal data for analysis and statistics using advanced analytical methods, such as machine learing and AI. We may do this if we have your consent, cf GDPR 6.1(a) 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 or to pursue our legitimate interest to set fees and prices in general, cf. GDPR art. 6.1 (f).
- When we carry out fraud detection on card and account transactions, including processing of behavioural 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, 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 research purposes as part of research projects or similar, including anonymisation 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, we do so if we have 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. GDPR, art. 6.1(a). We refer to our cookie policy for further information (Danske Bank's 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, cf. GDPR art. 6.1(c) and art 32.
- We use video surveillance and record the front of buildings, entrances to our branches and other premises, reception and customer areas, cash machines and counters where we are pursuing legitimate interests, cf. GDPR art. 6.1(f) and subject to the Swedish Act on Video Surveillance (kamerabevakningslag (2018:1200)).
- 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 adress 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).
- We may also invite you to events and send you marketing material in areas that we think may have your interest, and we track If you open the email incl. the newsletter based on our legitimate interest, cf. GDPR art. 6.1(f).
- 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, based on legal obligations*, cf. GDPR art. 6.1(c), in accordance with the Swedish Data Protection Act (lag (2018:218) med kompletterande bestämmelser till EU.s dataskyddsförordning) and Regulation with Supplementary Provisions to the EU's General Data Protection Regulation (förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning) or permitted by the Swedish Data Protection Agency.

*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 Swedish Banking and Financing Business Act (lag (2004:297) om bank- och finansieringsrörelse)
- the Danish Financial Business Act (lov om finansiel virksomhed
- the Swedish Anti-Money Laundering Act (lag (2017: 630) om åtgärder mot penningtvätt och finansiering av terrorism)
- the Swedish Act on Tax proceedings (skatteförfarandelag (2011:1244))
- the Swedish Bookkeeping Act (bokföringslag (1999:1078))
- the Swedish Consumer Credit Act (konsumentkreditlag (2010:1846))
- the Swedish Payments Act (lag (2010:751) om betaltjänster)
- the Swedish Marketing Practices Act (marknadsföringslag (2008:486)
- the General Data Protection Regulation (GDPR) and the Danish Data Protection Act (databeskyttelseloven), the Swedish Supplementary Data Protection Act (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning) and the Swedish Supplementary Data Protection Regulation (förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning)

- the Swedish Act on identification of reportable accounts for automatic exchange of information on financial accounts (lag (2015:911) om identifiering av rapporteringspliktiga konton vid automatiskt utbyte av upplysningar om finansiella konton)
- the Swedish Act on identification of reportable accounts due to the FATCA agreement (lag (2015:62) om identifiering av rapporteringspliktiga konton med anledning av FATCA-avtalet)
- the Swedish Capital Markets Act (lag (2007:528) om värdepappersmarknaden)
- the EU Markets in Financial Instruments Regulation (MiFIR)
- the EU Regulation on Market Abuse (the Market Abuse Regulation)
- the EU Capital Requirement Regulation (CRR) (Kapitalkravsförordningen)
- the Swedish Act on Video Surveillance (kamerabevakningslag (2018:1200))
- the EU Markets in Financial Instruments Regulations (MiFID I and II)
- the Swedish Enforcement Act (utsökningsbalk (1981:774))

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 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:

- We process sensitive personal data about you that may appear in budget and tax information you give us for credit evaluation purposes and transactions you ask us to initiate with your consent, cf. GDPR, art. 6.1(a) and 9.2(a).
- We process sensitive personal data about you when you provide us with information of your food preferences which may entail information about allergies or the like, i.e. if you participate in hospitality events we arrange with your consent, cf. GDPR, art. 6.1(a) and 9.2(a).
- For certain products or services, we may ask to process your sensitive personal data for the purpose of providing you with such a product or service 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) and 9.2 (g).
- 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 6.1(f) and 9.2(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

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

- you use our digital solutions or visit our websites
- you provide us with your household information
- we collect personal data from electronic communications, telephone and video recordings and monitoring
- you participate in hospitality events organized or hosted by us
- we track 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 according to the EU Markets in Financial Instruments Regulations (MiFID I and II). 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 calls 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, such as Meta or Google. We share responsibility (joint controllership) for such third parties' use of your personal data which is collected by way of cookies and processed for our benefit. We refer to our cookie policy (Danske Bank's cookie policy) for further information.

Personal data we collect from third parties

We receive and collect 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.
- Our corporate customer to which you have a relationship.
- The customer you have a connection with.
- 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.
- The Swedish State Personal Address Register (Statens personadressregister (SPAR)), the Swedish Companies Register (Bolagsregistret), the Swedish Real Property Register (Fastighetsregistret), National Board of Housing (Boverket) or other publicly accessible sources and registers.
- We process the data for example for identification and verification purposes and to update data and check personal data accuracy, cf. GDPR art. 6.1(f), chapter 3 section 10 of the Swedish Data Protection Act (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).
- Credit rating agencies and warning registers (e.g. UC AB).
- We collect and process the personal data, such as income, property holdings, existing credit and debt balance with the Swedish Enforcement Agency, to perform credit assessments. We update the personal data regularly.
- Other entities of the Danske Bank Group, if we have your consent, 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, such as the Capital Requirement Regulation (CRR) or sharing of notifications to the Swedish Financial Intelligence Unit (Finanspolisen) and Swedish Security Service (Säkerhetspolisen) in accordance with anti-money-laundering legislation.

- External data controllers, such as business partners (including correspondent banks, other banks and suppliers) 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 when mortgages are acquired or transferred.
- 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) and/or reporting requirements established by law or required by regulators.
- The Swedish Financial Intelligence Unit (Finanspolisen) and Swedish Security Service (Säkerhetspolisen) 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.
- For further information on the data protection practices of Swift in relation to the processing of your personal data in the context of the Swift Transaction Processing Services, please consult the Swift Personal Data Protection Policy (PDPP).
- 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 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.
- Guarantors, pledgers, individuals holding a power of attorney, lawyers, accountants, or others you have authorised us to share information with.
- If you have joint financial products with someone, such as a joint account we share your information, including personal identification number, with your co-product holder/owner and for tax reporting purposes.
- External business partners (including Nets, correspondent banks and other banks) 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 anti-money laundering, fraud, abuse and loss.
- Our suppliers, including, 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.
- Data processors: IT service providers (who may be located outside the EU and the EEA, such as Infosys Limited) and other service- and product suppliers like Bankgirocentralen BGC AB, Getswish AB, Finansiell ID – Teknik BID AB and Mastercard which all are important suppliers to the Swedish branch of Danske Bank.
- Social media companies, such as Meta and Google when you have given your consent for direct marketing purposes.
- Public authorities as required by law or according to court orders. This could for example include the Swedish Police (Polisen), the Swedish Prosecution Authority (Åklagarmyndigheten), the Swedish Financial Intelligence Unit (Finanspolisen), the Swedish Security Service (Säkerhetspolisen), in a accordance with the Swedish Banking and Financing Business Act (lag (2004:297) om bank- och finansieringsrörelse) or the the Swedish Anti-Money

Laundering Act (lag (2017: 630) om åtgärder mot penningtvätt och finansiering av terrorism), the Swedish tax authorities (Skatteverket) in accordance with the Swedish Act on Tax Proceedings (skatteförfarandelagen (2011:1244)), the Enforcement Authority in accordance with the Swedish Enforcement Act (utsökningsbalk (1981:774)) and the Swedish central bank (Sveriges Riksbank) for statistical and other purposes.

- Regulators, such as the Danish and Swedish Financial Supervisory Authority (DK: Finanstilsynet, SE: Finansinspektionen), the Data Protection Agency (Integritetsskyddsmyndigheten), law enforcement agencies and authorities in Sweden or abroad in connection with their duties.
- Credit rating agencies. If you are granted a loan or default on your obligations to Danske Bank, we report you to credit rating agencies and/or warning registers (UC AB) 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.
- If you activate the account information function in your smart phone it´s possible that your internet-, tele- or OS supplier like Google or Apple can view the information.
- 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, other external data and 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 Danske Bank's 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 decisions are quicker and more fair, efficient and correct than decisions made through a similar manual process.

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.

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, 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 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 defence 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 Swedish Data Protection Agency's website: http://www.imy.se
- on the EU Commission's website: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

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 anonymised.

We have many different processes where we use your personal data and many different legal bases for retention of your personal data. Our 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 account information for up to eleven years so we may defend our legal rights within statutory limitation periods.
- We keep your Know Your Customer information (KYC) for as long as you are a customer and for an additional five years as required by the Swedish Anti-Money Laundering Act.
- We keep credit and collateral agreements for up to eleven years after expiry to document our agreement so we may defend our legal rights within statutory limitation periods.
- If you have a credit product in the bank, we keep your credit information for as long as you are a customer and for seven years after termination of our customer relationship.
- We keep your consent to our use of cookies for one year unless you withdraw it earlier.
- In one circumstance, we keep your personal data for a period of up to 30 years. This is exclusively for use in our Internal Ratings Based (IRB) models used for the bank's risk management and calculation of capital requirements under the Capital Requirements Regulation (CRR) and where we are required to document financial crises cycles .
- We keep your voice recordings for different purposes. We have a legal obligation to keep voice recordings related to investments services for five years under MiFID and voice records that constitute bookkeeping material for seven years after the recording year under the Swedish Bookkeeping Act.
- We also keep voice recordings containing assignments for eleven years for document purposes so we may defend our legal rights within statutory limitation periods. Reference is made 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).
- 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 Swedish Anti-Money Laundering Act.
- Surveillance videos are deleted 30 days after they were made in accordance with relevant legislation. In case of a police investigation, the video may be stored for a longer period.

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:

- Make a request online to receive an overview of your personal data at [Request an overview of your personal data]
- Contact us on our main telephone number +46 752 48 45 42.
- 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 write to GDPR-insight@danskebank.se. However, you may also contact us via your adviser or via message in Danske eBanking or Danske Mobile Banking.

In the Profile section of Danske Mobile Banking, you can also get an overview of the most common data we process about you, and you can update your personal 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, the right to erasure shall not apply to the extent the processing is necessary:

- 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 Swedish Anti-Money Laundering Act or the Swedish Bookkeeping 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 Swedish central bank (Sveriges Riksbank).
- For establishment, exercise, or defence 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 Danske Bank (see the beginning of this section 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 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. On your request, if secure and technically possible, we can 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 (+46 752 48 45 42) 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, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark.

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

You can contact our data protection officer with all questions on our use of your personal data. 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: Danske Bank, Klagomålsansvarig, Box 328, 581 03 Linköping. You can also lodge a complaint with the Swedish Data Protection Authority: Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm, imy@imy.se. If, for example, your residence or the place of the alleged infringement is in or is related to another member state than Sweden, 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.