

# Privacy notice for all individuals

## Danske Bank A/S, Danmark, Sverige Filial Danske Hypotek AB

Effektive from 1 October 2020

### 1. Introduction

This privacy notice applies to the processing of personal data by the Swedish branch of Danske Bank A/S ("Danske Bank A/S, Danmark, Sverige Filial").

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.

#### Data controllers:

Danske Bank A/S 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 is in that situation the data controller and Danske Bank A/S is the processor.

#### Contact details:

Danske Bank A/S, CVR.no. 61126228 (Erhvervsstyrelsen)  
Holmens Kanal 2-12, DK-1092 København K.

Danske Bank A/S, Danmark, Sverige Filial, Corporate Identity No. 516401-9811 (Bolagsverket), Box 7523, 103 92 Stockholm.

Danske Hypotek AB (publ), Corporate Identity No. 559001-4154 (Bolagsverket), Box 7523, 103 92 Stockholm.

More information about the data controllers and the Swedish branch is available on the respective websites: [www.danskebank.se](http://www.danskebank.se), [www.danskebank.dk](http://www.danskebank.dk) and [www.danskehypotek.se](http://www.danskehypotek.se).

When "Danske Bank" or "we" is used below it includes both Danske Bank A/S and Danske Hypotek AB'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, employees or owners of a corporate

customer and other individuals with whom we interact and collaborate with.

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

### 2. What personal data do we process?

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

- personal details including your name, social security number or other national ID number, citizenship, country of residence, tax residence, tax identification number and identification documentation such as copies of your passport, driver's licence and birth certificate,
- contact information, including your address, telephone number and email address,
- financial information, including details about your income and expenses, assets, debt, credit rating and insurances,
- information about collateral, including market value, energy data and environmental aspects,
- information about your education, profession, work, knowledge and experience,
- information about your investment targets,
- information about your family and household,
- information if you as our private customer also is an entrepreneur,
- details about the services and products we provide to you, including amongst others accounts, cards, loans, credits, etc.,
- transaction data,
- how you use our services and products and your preferences towards them,
- digital information related to your use of our websites, platforms and digital applications, including traffic data, location data, behavioural data and other communication data,
- information related to the devices you use to access our websites as well as technical information, including the type of device and operating system,
- information provided by you about your preferences for various types of marketing and events,
- information about your visits to our premises, and
- telephone conversations with you.

We will 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 keep us updated on any changes.

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

We process data about you to provide the best advice and solutions, keep your finances safe and fulfil our agreements with you.

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
- loan and credit
- digital banking solutions
- investment services and advice
- insurance and pension services

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 service and managing the customer relationship, including advice, administration, credit assessment, recovering of outstanding debt, handling of complaints and to make information available to service providers who are authorized to request your information.
- Communicating with you about your products and services for legal, regulatory and servicing purposes.
- To improve, develop and manage our products and services and setting fees and prices for our products and services, including use of data analytics and statistics to improve products and services and to test our systems.
- For marketing of our services and products, including marketing on behalf of other entities in the Danske Bank Group or our partners, if we have your permission or if we are allowed to by law. We use cookies and similar technology on our website, including for marketing via digital channels and social media platforms such as Facebook. We refer to our cookie policy for further information <https://danskebank.se/behandling-af-personoplysninger-og-cookies>.
- To comply with applicable law and for other regulatory and administrative purposes, including identification and verification according to anti-money laundering legislation, risk management and prevention and detection of money laundering, fraud and other types of financial

crime. In relation to anti-money laundering, identification data is collected at regular intervals during your agreement with us as required by law.

- For security purposes, including use of video surveillance of ATMs, entrances to our branches and other premises.

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

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

- you have granted us consent to use your personal data for a specific purpose, cf. the General Data Protection Regulation (GDPR) art. 6.1(a),
- you have made or you are considering making an agreement with us for a service or product, cf. GDPR art. 6.1(b),
- to comply with a legal obligation, cf. GDPR art. 6.1(c), for example, in accordance with
  - The Swedish Anti-Money Laundering Act (*Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism*)
  - The Swedish Act on Tax proceedings (*Skatteförfarandelagen (2011:1244)*)
  - The Swedish bookkeeping Act (*Bokföringslagen (1999:1078)*)
  - The Swedish Consumer Credit Act (*Konsumentkreditlagen (2010:1846)*)
  - The Danish Financial Business Act (*Lov om finansiel virksomhed*) and the Swedish Banking and financing Business Act (*Lag (2004:297) om bank- och finansieringsrörelse*)
  - The Swedish Payments Act (*Lag (2010:751) om betaltjänster*)
  - General Data Protection Regulation (GDPR) and The Danish and the Swedish Data Protection Act (*Databeskyttelsesloven och Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*)
  - The Swedish Capital Markets Act (*Lag (2007:528) om värdepappersmarknaden*)
  - The Swedish Act on identification of reportable accounts for automatic exchange of information on financial accounts (2015:911) (*Lagen 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 (2015:62) (*Lagen om identifiering av rapporteringspliktiga konton med anledning av FATCA-avtalet*)
- it is necessary to pursue a legitimate interest of Danske Bank, cf. GDPR art. 6.1(f). For example, this may be for documentation and security purposes, to prevent and detect money laundering, to prevent and detect fraud, abuse and loss, to strengthen IT and payment security and for direct marketing purposes. We also use legitimate interest as legal basis, when we process data about

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

## 5. Sensitive personal data

Some of the information we hold about you might 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,
- information about your health and your genetic background, e.g. inherited health qualities,
- biometric data, e.g. via facial recognition technology,
- information about your religious or philosophical beliefs, and
- information about your political opinions.

We also process sensitive personal data that may appear in budget and tax information you give us and transactions you ask us to initiate.

### Purposes for processing sensitive personal data

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

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

### Legal basis for processing sensitive personal data

Our processing of your sensitive personal data can be on the legal basis of:

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

## 6. How do we collect information we hold about you?

### Personal data collected from you

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

- fill out applications and other forms for ordering services and products,
- submit specific documents to us,

- participate in meetings with us, e.g. with your advisor,
- talk to us on the phone,
- use our website, mobile applications, products and services,
- participate in our customer surveys or promotions organised by us, and
- communicate with us via letter, electronic means, including e-mails, or social media.

### Voice recordings:

When you call us or when we call you at your request or to follow up on your inquiry, conversations may be recorded and stored due to documentation and security purposes. Before an employee answers the call or before you enter the queue, you will be notified if the call will be recorded. In few situations, e.g. in case of long waiting time, your call can though be redirected to a non-recorded employee without notifying you. If we talk with you about investment services, we are obliged to record and store our telephone conversation.

### Personal data collected from third parties

We receive and collect data from third parties, including from:

- Shops, banks, payment and services providers when you use your credit or payment cards, Danske eBanking or other payment services. We process the data to execute payments and prepare account statements, payment summaries and the like.
- If you have a joint account with someone, we may collect information about you and your joint account from your co-account holder.
- The Swedish State Personal Address Register (Statens personadressregister (SPAR)), the Swedish Companies Register (Bolagsregistret), the Swedish Real Property Register (Fastighetsregistret), National Board of Housing (Boverket) and other publicly accessible sources and registers. Sometimes we collect these data via other third parties which provides them. We process the data, for e.g. identification and verification purposes and to check data accuracy.
- Credit rating agencies and warning registers (e.g. UC AB). We process the data to perform credit assessments. We update the data regularly.
- Other entities in the Danske Bank Group if we have your consent, e.g. to provide you with better customized products and services.
- Other entities within Danske Bank Group if existing legislation allow or require us to share the information, e.g. if it is necessary to comply with group-based management, control and/or reporting requirements established by law, or sharing of notifications to the Swedish Financial Intelligence Unit and Swedish Security Service in accordance with anti-money-laundering legislation.
- External business partners (including 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, to enable our customers to use banking services abroad, or to prevent and detect money laundering fraud, abuse and loss.

- The customer you have a connection with.

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

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

- Other entities in the Danske Bank Group if we have your consent, e.g. to provide you with better customized products and services.
- Other entities within Danske Bank Group if existing legislation allow or require us to share the information, e.g. if it is necessary to comply with group-based management, control and/or reporting requirements established by law, or sharing of notifications to the Swedish Financial Intelligence Unit and Swedish Security Service 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 who are authorized as an account information service, payment initiation service, or card-based payment instrument provider, if you (or someone who via our online services can view information about your accounts or initiate payments on your behalf) request such a service provider to receive information about you.
- Guarantors, pledgers, individuals holding a power of attorney, lawyers, accountants or others you have authorised us to share the information with.
- If you have a joint account with someone, we may share your information with your co-account holder.
- External business partners (including correspondent banks 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 and consultants.
- Data processors including IT service providers who may be located outside the EU and the EEA, such as Danske Bank India. Bankgirocentralen AB (<https://www.bankgirot.se/om-bankgirot/kontakt-oss/behandling-av-personuppgifter/>) and Finansiell ID – Teknik BID AB (BankID- <https://www.bankid.com/licensavtal/privacy-statement>) are examples of two important suppliers to Danske Bank Sweden.
- Social media companies such as Facebook.
- Public authorities as required by law or according to court orders or requests from the police, the bailiff, tax

authorities or other authorities. This could include the Swedish Financial Intelligence and Swedish Security Service in accordance with the Swedish Anti-Money-Laundering Act, the Swedish Tax Authorities in accordance with the Swedish Tax Proceedings Act and the Swedish central bank (Riksbanken) for statistical and other purposes.

- Regulators, e.g. the Danish and the Swedish Financial Supervisory Authority (DK: Finanstilsynet SE: Finansinspektionen), law enforcement agencies and authorities in Sweden and in other countries, including outside the EU and the EEA, in connection with their duties.
- Credit rating agencies. If you default on your obligations to Danske Bank, we may report you to credit rating agencies and/or warning registers (UC AB) in accordance with applicable law.
- If you activate the payment information function in your smart phone it's possible that your internet-, tele- or OS supplier like Google or Apple can view the information.
- 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 Australia, Canada and India.

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

- ensuring that there is an adequacy decision by the European Commission, or
- 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, value assets and for marketing purposes.

### Automated decision-making

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

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

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

In relation to 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 completing a payment that is likely to be fraudulent.

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

### 10. How long do we store your personal data?

We keep your data only for as long as it is needed for the purpose for which your data were registered and used.

When your business connection with us has terminated, we normally keep your data for a further 7 years. This is primarily due to our obligations under the Bookkeeping Act, the Anti-Money Laundering Act and requirements from the Financial Supervisory Authority. In certain circumstances, we keep your information for a longer period of time. This is the case for example:

- if your personal information form part of our calculation of our capital requirements, then we may keep your information for up to 20 years,
- if the statute of limitation is 10 years, then we may keep your data for up to 10 years, and
- if required to due to other regulatory requirements.

If you as a potential new customer have asked for an offer for a loan or another product or service but refuses 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 the Anti-Money Laundering Act.

### 11. Your rights

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

- make a request online at [www.danskebank.se/gdpr-formular](http://www.danskebank.se/gdpr-formular),
- contact us via our main telephone number 0752-48 45 42, or
- if you have a personal advisor, contact your advisor directly.

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

### Right to access your personal data

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

Under the "Profile" section of the mobile bank app, you can obtain an overview of the personal data you have given us. You will find your contact information and information you have given us about your household, income, debt and so on. You can update the information if changes have occurred in your life.

You can make an access request via the mobile bank app or our webpage at [www.danskebank.se/gdpr-formular](http://www.danskebank.se/gdpr-formular).

### Rights related to automated decision making

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

### Right to object

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

### Objection to direct marketing

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



### Direct Marketing Block

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

### Right to rectification of your data

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

### Right to erasure ('right to be forgotten')

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

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

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

### Restriction of use

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

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

### Withdrawal of consent

Where consent is the legal basis for a specific processing activity, you can withdraw your consent at any given time. Please note that 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 we are required to do so by law.

### Data portability

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

### 12. Changes to the 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 are processed will have a significant effect on you personally, we will take reasonable steps to let you know of the changes to allow you to exercise your rights (for example, to object to the processing).

### 13. Contact details and how can you complain

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

You can contact us via our main telephone number 0752-48 45 42. You are also welcome to contact your advisor directly.

You can contact our Data Protection Officer via email [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: Danske Bank, Legal Department, Box 7523, 103 92 Stockholm. You can also lodge a complaint with the Swedish Data Protection Agency: Datainspektionen, Box 8114, 104 20 Stockholm, e-mail: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se).