Danske Bank A/S Hamburg Branch privacy notice for business customers

Effective from 22-02-2020

1. Introduction

This privacy notice applies to the processing of personal data by the Hamburg Branch of Danske Bank A/S (Danske Bank Hamburg). Danske Bank A/S (Danske Bank) is the data controller for the processing of the personal data comprised by this privacy notice.
Contact details:
Danske Bank A/S, CVR no. 61126228, Holmens Kanal 2-12, DK-1092 København K, Denmark;
Danske Bank A/S Zweigniederlassung Hamburg, AG Hamburg HRB 33810, Spitalerstraße 22-26, 20095 Hamburg.

In the course of our business, we process information about you (personal data).

This privacy notice applies to individuals who are connected with a business customer of Danske Bank Hamburg. You may be an authorised signatory, a beneficial owner, a director, an employee, a guarantor, a pledgor or another third party connected with a business customer served by Danske Bank Hamburg.

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 connection with our business customer, we process different types of personal data, including

- personal details such as your name, place and date of birth, citizenship, resident address, social security number or other national ID number, German tax identification number and proof of identity such as a copy of your passport, ID card, driver's licence and birth certificate and authetification data such as a sample of your signature,
- contact information, including your business address, telephone number and email address,
- information about your employer, education, profession, work, knowledge and experience
- details about the services and products we provide to you, including accounts, cards and access rights,
- how you use our services and products and your preferences in relation to them,
- digital information related to your use of our websites, platforms and digital applications, including, traffic data, location data, behavioural data and other communication data,
- information about the devices you use to access our websites as well as technical information, including the type of device and operating system,
- information provided by you about preferences for various types of marketing and events,
- information about your visits to our premises including video surveillance, and
- telephone conversations with you.

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

3. What we use your personal data for

Danske Bank may process your personal data for any of the following purposes, depending on the capacity in which you interact with us:

- For potential customers to be able to offer relevant products and services, and, if they choose to accept one or more of our products or services and become a customer, for onboarding purposes in relation to identification and verification for anti-money laundering purposes.
- Customer services and customer relationship management, including advice, administration, management of employee corporate cards, recovery of outstanding debt, handling of complaints and to make information available to service providers authorised to request information about you.
- Communicating with you about your products and services for legal, regulatory and servicing purposes.
- To improve, develop and manage our products and services and setting fees and prices for our products and services, including using data analytics and statistics to improve products and services and to test our systems.
- Marketing of our services and products, including marketing on behalf of other entities of the Danske Bank Group or our partners, if we have your permission for this or are allowed such marketing by law. We use cookies and similar technology on our website, including for marketing via digital channels and social media platforms such as Facebook. Please refer to our cookie policy for further information.
- To comply with applicable law and for other regulatory and administrative purposes, including identification and verification according to anti-money laundering legislation, risk management, and prevention and detection of money laundering, fraud and other types of financial crime. In relation to anti-money laundering, identification data is collected at regular intervals during our business customer's relationship with us as required by law.
- Security, including the use of video surveillance of the front of buildings, entrances to our premises.

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

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

- You have given us consent to use your personal data for a specific purpose, cf. the GDPR, art. 6.1(a)
- You have entered into or are considering entering into an agreement with us on a service or product, cf. the GDPR, art. 6.1(b)
- To comply with a legal obligation, cf. the GDPR, art. 6.1(c), for example, in accordance with
    - the German Anti-Money Laundering Act (*GWG*)
    - the German Banking Act (*KWG*)
    - the German Tax Code (*AO*)
    - the German Capital Investment Code (*KAGB*)
    - the German Securities Trading Act (*WpHG*)
    - the German Payments Services Supervision Act (*ZAG*)
    - the German Commercial Code (*HGB*)
    - the German Data Protection Act (*BDSG*)
    - the Danish Anti-Money Laundering Act (*hvidvaskloven*)
    - the Danish Tax Control Act (*skattekontrolloven*)
    - the Danish Bookkeeping Act (*bogføringsloven*)
    - the Danish Credit Agreements Act (*kreditaftaleloven*)
    - the Danish Financial Business Act (*lov om finansiel virksomhed)*
    - the Danish Payments Act (*betalingsloven*)
    - the Danish Data Protection Act (*databeskyttelsesloven*)
    - the Danish Capital Markets Act (*lov om kapitalmarkeder*)
    - the Danish CPR Act *(CPR-loven)*
- It is necessary to pursue Danske Bank's or another third party's legitimate interest, cf. the GDPR, art. 6.1(f). For example, if Danske Bank or the business customer that you have a connection with has a business or commercial reason, such as administration of the services and products that the customer has requested, to give you the required access to digital services, for documentation and security purposes, to prevent and detect money laundering, to prevent and detect fraud, abuse and loss, to strengthen IT and payment security and for direct marketing purposes. We will do so only if our legitimate interest in each case is not outweighed by your interests or rights and freedoms.

If you shall represent a legal entity that is our customer, you are obliged to provide us with such personal data necessary to (i) commence or execute a representation and to comply with the contractual obligations of the specific contractual relationship or (ii) to comply with

our regulatory obligation. Without such personal data we will in general have to decline or seize to accept you as representative. Especially, under anti-money laundering regulation we are obliged to identify you by using e.g. your ID card and to collect and store your name, date and place of birth, nationality and residential address. In order to enable us to comply with this obligation, pursuant to sec. 11~~4~~ para. 6 of the German Anti-money laundering Act you have to provide us with the necessary information and documentation and have to inform us on any changes in the course of the business relationship immediately. If you do not provide the necessary information and documentation, we are not allowed to implement or continue to accept your authorization as requested by the business customer you shall represent.

5. Sensitive personal data

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

Types of sensitive personal data
In particular, we may process biometric data, for example via facial recognition technology.

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

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

- for the purpose of a product or service we provide to you or the business customer that you have a connection with,
- for identification and verification purposes,
- for the prevention and detection of money laundering and other types of crime, including for fraud prevention and detection purposes, and
- to comply with legal requirements that apply to us as a financial institution.

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

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

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

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

- fill in applications and other forms for ordering services and products,
- submit specific documents to us,
- participate in meetings with us, for instance as a representative of the business customer that you have a connection with,
- 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 and digital means, including e-mails, or social media.

Voice recordings
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

- The business customer that you have a connection with.
- Shops, banks and payment and service providers when you use your credit or payment cards, Danske eBanking, District or other payment services. We process the data to execute payments and prepare account statements, payment summaries and the like.
- The German Trade Register and Companies Register (*Handelsregister* and *Unternehmens-register*), the Danish Central Office of Civil Registration (*CPR-kontoret*) and other publicly accessible sources and registers. We process the data, for example for identification and verification purposes and to check data accuracy.
- 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, or the sharing of notifications to the State Prosecutor for Serious Economic and International Crime (*SØIK*) or German law enforcement authorities in accordance with anti-money laundering legislation.
- External business partners (including correspondent banks and other banks) 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.

7. Third parties that we share your personal data with

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

- Other entities of the Danske Bank Group if we have your consent, for example to provide you with better customised products and services.
- Other entities of the Danske Bank Group if existing legislation allows or requires us to share the information, for example if it is necessary to comply with group-based management, control and/or reporting requirements established by law, or the sharing of notifications to German law enforcement authorities or the State Prosecutor for Serious Economic and International Crime (*SØIK*) in accordance with anti-money-laundering legislation.
- Service providers authorised as an account information service, payment initiation service or card-based payment instrument provider, when the service provider duly requests information about the account belonging to the business customer with which you are connected.
- Guarantors, individuals holding a power of attorney, lawyers, accountants or others you have authorised us to share the information with.
- External business partners (including correspondent banks and other banks) if we have your consent or if permitted under existing legislation, for example to prevent and detect money laundering, fraud, abuse and loss.
- Our suppliers, including lawyers, accountants, consultants and courier services. We use courier services to deliver, for example, credit cards to you, and we disclose your name, address and telephone number to them, so you can receive the consignment.
- Data processors, including IT service providers who may be located outside the EU and the EEA, such as Danske Bank India.
- Social media companies, such as Facebook.
- 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 State Prosecutor for Serious Economic and International Crime (*SØIK*) in accordance with the Danish Anti-Money Laundering Act and the German Financial Intelligence Unit (*FIU*) in accordance with the German Anti-Money Laundering Act, to the Danish tax authorities in accordance with the Danish Tax Control Act and the German tax authorities in accordance with the German Tax Act and the Danish central bank (*Danmarks Nationalbank*) and Central Bank (*Deutsche Bundesbank*) in accordance with the German Banking Act and for statistical and other purposes.
- Regulators, such as the Danish Financial Supervisory Authority (*Finanstilsynet*) and the German Financial Supervisory Authority (*BaFin*), law enforcement agencies and authorities in Denmark, Germany and other countries, including countries outside the EU and the EEA, in connection with their duties.
- For social and economic research or statistics purposes, where it is in the public interest.

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

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

When Danske Bank transfers your personal data to third parties outside the EU and the EEA, we ensure that your personal data and data protection rights are subject to appropriate safeguardings by

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

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

9. Profiling and automated decisions

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

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

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

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

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

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

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

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

We keep your data only for as long as it is needed for the purpose for which your data was processed.

When your relations with us have terminated, or when the business relationship with the business customer that you have a connection with has terminated, we normally keep your data for another seven years. This is due primarily to our obligations under the Danish Bookkeeping Act, the Danish Anti-Money Laundering Act and requirements from the Danish Financial Supervisory Authority as well as the German Commercial Code, the German Tax Act, the German Anti-Money Laundering Act, the German Banking Act and requirements from the German Ministry of Finance or German 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 forms part of the 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,
- if required due to your connection with our business customer, and
- if required due to other regulatory requirements.

If the business you are connected with as a potential customer has asked for a loan offer or another product or service, but refuse the offer and do not become a customer, 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 German and Danish Anti-Money Laundering Acts.

Surveillance videos are deleted 30 days after they were made in accordance with applicable law. In certain circumstances, and in connection with a specific case, the information may be stored for a longer period.

11. Your rights

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

- make a request online at danskebank.dk/gdpr
- contact us on our main telephone number +49 40 32 81 16 0
- contact your adviser directly if you have one

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

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

You can make an access request via our webpage at danskebank.dk/gdpr.

Rights related to automated decision-making
You can obtain information on how an automated decision was made and the effects of the decision, you can express your point of view, you can object to the decision, and you can request a manual review of any automated decision.

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

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

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

Right to erasure ('right to be forgotten')
You are entitled to have your data erased, if the data is no longer necessary in relation to the purposes for which it was collected.
However, in the following cases, we may or are required to keep your data:

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

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

Withdrawal of consent
Where consent is the legal basis for a specific processing activity, you may withdraw your consent at any time with future effect. Please note that if you withdraw your consent, we may not be able to offer you specific services or products. Note also that we will continue to use your personal data, for example to fulfil an agreement we have made with you or if we are required by law to do so.

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

12. Changes to this privacy notice

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

13. Contact details and how to complain

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

You can contact us on our main telephone number in Germany +49 40 32 81 16 0. You are also welcome to contact your adviser directly.

You can contact our Data Protection Officer by email at 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, Holmens Kanal 2-12, DK-1092 København K, email: klageservice@danskebank.dk.

You can also lodge a complaint with a data protection supervisory authority, in particular in the member state of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of personal data relating to you infringes with GDPR in connection with sec. 19 German Data Protection Act.

Information on your right to object under article 21 of the EU General Data Protection Regulation (GDPR)

1. Ad hoc right to object

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on article 6 (1) e) GDPR (processing in the public interest) and article 6 (1) f) GDPR (processing for the purposes of safeguarding legitimate interests).

If you lodge an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or unless the processing is for the establishment, exercise or defence of legal claims.

2. Right to object to the processing of data for marketing purposes

In certain cases, we process your personal data for direct marketing purposes. You have the right to object at any time to processing of personal data concerning yourself for such marketing, which includes profiling to the extent that it is related to such direct marketing.

If you object to processing for direct marketing purposes, we will no longer processes your personal data for such purposes.

There are no formal requirements for lodging an objection.