Danske Bank A/S, London Branch privacy notice

Effective from September 2024

1. Introduction

This privacy notice applies to the processing of personal data of individuals who are related to customers, clients, agents or counterparties of Danske Bank A/S, London Branch. You may, as an example, be an authorised signatory, beneficial owner, director, employee, guarantor or other third party related to a customer, client, agent or counterparty of ours. Danske Bank is the data controller for the processing of the personal data covered by this privacy notice. Contact details: Danske Bank A/S, London Branch, company number: FC011846, 4th Floor, 75 King William Street, London EC4N 7DT.

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

Data Protection Officer
Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark
Email address: dpofunction@danskebank.dk

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

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

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

2. What personal data do we collect and process?

Depending on your connection with our customer, client, agent or counterparty we collect and process different types of personal data, including:

- identification information, such as your name, social security number or other national ID number and proof of identity such as a copy of your passport, driver's licence and birth certificate
- contact information, including your address, telephone number and email address
- information about your education, profession, work, knowledge and experience
- details about the services and products we provide to you or to our customer, client, agent or counterparty, 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, to the extent applicable and necessary, traffic data, location data, behavioural data and other communication data, e.g. by using cookies and similar technology on our website (see also: Cookie policy (danskeci.com)
- information about the devices you use to access our websites as well as technical information, including the type of device and operating systems
- information provided by you about preferences for various types of marketing and events
- tracking data if you have consented to this in connection with signing up for receiving newsletters
- information about your visits to our offices, including video surveillance
- recordings of telephone conversations and online meetings with you
- other personal data as necessary to provide you or our customer, client, agent or counterparty with specific products, services or transactions or which we are required by law to collect and process.

Our ability to offer the best possible advice and solutions for you and our customers, clients, agents and counterparties very much depends on how accurate the information you provide is and on you informing us of any changes to this information.

3. Why and on which legal basis we process your personal data

• When we onboard you as a user of an online product or platform for a customer, client or counterparty, we process your personal data for both identification, verification and for anti-money laundering purposes. The legal basis for this processing is to comply with a legal obligation, (see: (Retained EU Legislation) Regulation (EU) 2016/679 (United Kingdom General Data Protection Regulation) (UK GDPR) article 6.1(c)) for example, pursuant to The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Money Laundering Regulations)

• When we provide our customer, client or counterparty with a financial product you have requested or consider to obtain on behalf of our customer, client or counterparty (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 within 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 or our customer, client or counterparty) we do this because you or our customer, client or counterparty have entered or consider entering into an agreement with us on delivery of a service or product (see UK GDPR article 6.1(b)) and to pursue legitimate interests (see UK GDPR article 6.1(f))

• Sometimes we share your personal data with another company within the Danske Bank Group or transfer your personal data to a third party so you may receive a quotation for a product or a service because we have agreed to do so with our customer, client or counterparty (see UK GDPR article 6.1(b)) and in relation to the transfer of your personal data we pursue legitimate interests (see UK GDPR article 6.1(f)) or you may have given us consent to use and share your personal data for such specific purposes yourself (see UK GDPR article 6.1(a))

• When we communicate with you about the products and services you have requested or send you information on our system updates, we do so to fulfil a contract with you (see UK GDPR article 6.1(b)) or subject to a legal obligation (see UK GDPR article 6.1(c)) or to pursue a legitimate interest (see UK GDPR article 6.1(f))

• When we improve, develop, and manage our IT-systems we may, if necessary, use your personal data to improve or develop products and services and test our systems or develop, train and test IT- and other models. This may be done on the legal basis we have for processing your personal data in our IT-systems in the first instance (which could be any of the legal bases mentioned in this section), and/or to ensure a sufficient level of security (see UK GDPR article 6.1(c) and UK GDPR article 32) or we may pursue a legitimate interest (see UK GDPR article 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 (see UK GDPR article 6.1(b)) so you on behalf of our customer, client or counterparty may receive a price quotation or a product offering and in relation to processing your personal data we pursue a legitimate interest (see UK GDPR article 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, as well as detection and prevention of fraud, credit fraud and other types of financial crimes, we do so to comply with legal obligations (see UK GDPR article 6.1(c)) and to pursue legitimate interests (see UK GDPR article 6.1(f))

• When we pursue statistical, scientific, and/or research purposes as part of research projects or similar, including anonymisation of personal data for such purposes, we pursue legitimate interests (see UK GDPR article 6.1(f)) or we act in the public interest (see UK GDPR article 6.1(e))

• When we carry out profiling and marketing of our services and products, including marketing on behalf of other legal entities of the Danske Bank Group, we do so if we have your consent for this (see UK GDPR article 6.1(a)) or we pursue legitimate interests (see UK GDPR article 6.1(f))

• When we use cookies and similar technology on our website and in our apps for functional, statistical and for marketing purposes via digital channels and social media platforms if you have consented to this (see UK GDPR article 6.1(a)). We refer to our cookie policy for further information please see: Cookie policy (danskeci.com))

• 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 (see UK GDPR article 6.1(c)) and to pursue legitimate interests of Danske Bank (see UK GDPR article 6.1(f))

• We process your personal data for security reasons (see UK GDPR articles 6.1(c) and 32)

• We use video surveillance and record such of the front of buildings, entrances to our branch, reception and customer areas, where we are pursuing legitimate interests (see UK GDPR article 6.1(f))

• When we collect, share, and use personal data to build, maintain, and use models for credit risk exposure and Internal Based Rating (IRB) modelling to assess capital requirements, we do so with reference to the Capital Requirements Regulation (CRR) which is required as part of the Bank's risk management (see UK GDPR article 6.1(c))

• When we send you newsletters, we process your personal data and we use your email and name for documentation purposes to send you articles, news, and updates because you have requested this service from us (see UK GDPR article 6.1(b)). We may also invite you to events and send you marketing material in areas which we think may have your interest and we track which articles have your interest and which you open, based on your consent (see UK GDPR article 6.1(a))

• We also carry out several other legal, regulatory, administrative, and compliance related processing activities which entail processing of personal data, including identification, and verification according to anti-money laundering legislation, risk management (see UK GDPR article 6.1(c)) and to pursue the legitimate interests of Danske Bank (see UK GDPR article 6.1(f))

When we refer to processing of your personal data due to "legal obligations" it refers to legal requirements in any of the following legislation (please note that this list is not exhaustive):

- Money Laundering Regulations
- Criminal Finances Act
- Financial Services & Markets Act
- Bribery Act
- Terrorism Act
- Proceeds of Crime Act
- UK Market Abuse Regulation
- UK Markets in Financial Instruments Regulations

4. 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
We may process the following types of sensitive personal data:

- Information about your health (e.g. information about access arrangements, dietary requirements or allergies for events)
- 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 customer, client, counterparty or agent 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
- 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 (see UK GDPR article 9.2(a)),
- the establishment, exercise or defence of legal claims (see UK GDPR article 9.2(f), or
- substantial public interest (see UK GDPR article 9.2(g).

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

Personal data collected from you
We collect information you share with us or by observing your actions, including, for example, when you

- fill in applications and other forms for ordering services and products
- submit specific documents to us
- participate in meetings with us
- talk to us on the phone
- use our website, mobile applications, products and services
- participate in our customer surveys or promotions organised by us
- communicate with us via letter and digital means, including e-mails, or social media
- use our digital solutions and Apps or visit our websites
- personal data collected from electronic communication, telephone and video recording and monitoring
- participate in hospitality events organised or hosted by us
- tracking on your subscription to newsletters

We are obliged under the UK Markets in Financial Instruments Regulations to monitor and store all electronic communications related to investment services, for instance when we chat, email or speak on the phone with you. We store this information for as long as we are legally required to. Incoming and outgoing calls may be recorded, listened to and stored for compliance with these regulatory requirements but also for documentation purposes.

Personal data collected from use of cookies
We 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 cookies that are needed to enable you to use our services (necessary cookies). If you consent to additional cookies, such as functional, statistical and/or marketing cookies, we will set cookies according to your choice to measure, analyse and improve the use and performance of our products and services and, to the extent applicable and relevant, to tailor and send you relevant marketing messages.

Some of the marketing cookies are owned by third parties, e.g. Meta or Google. We share responsibility (joint controllership) for such third parties' use of your personal data which is collected by use of cookies and processed for our benefit. Please refer to our cookie policy for further information (see: Cookie policy (danskeci.com)).

Personal data collected from third parties
We receive and collect personal data from third parties, including from

- The customer, client, counterparty or agent that you have a connection with.
- Shops, banks and payment and service providers when you use District or other payment services. We process the personal data to execute payments and prepare account statements, payment summaries and the like.
- Asset managers when we provide trade reports to their customers.
- Credit rating agencies and warning registers. We process the data to perform credit assessments. We update the 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, or the sharing of notifications to the National Crime Agency in accordance with anti-money laundering legislation.
- External data controllers such as business partners (including correspondent banks and other banks) and vendors if we have your consent or if permitted under existing legislation, for example to provide you or our customer, client, counterparty or agent 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 but we may share necessary personal data with group companies and third parties where we have an appropriate legal basis and where those group companies and third parties are also obliged to keep your personal data confidential. Some of the examples of this are set out below:

- 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 National Crime Agency 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 customer with which you are connected.
- Guarantors, individuals holding a power of attorney, lawyers, accountants or others you or the customer, client, counterparty or agent with which you are connected, have authorised us to share the information with.
- External data processors, 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.
- Data processors, including other units of the Danske Bank Group and IT service providers who may be located outside the UK, 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 or other

authorities. This could include the National Crime Agency.
- Regulators, such as the Prudential Regulation Authority and the Financial Conduct Authority, law enforcement agencies and authorities in the UK and other countries in connection with their duties.
- Credit rating agencies. If you default on your obligations to Danske Bank, we may report you to credit rating agencies and/or warning registers in accordance with applicable law.
- For social and economic research or statistics purposes, where it is in the public interest.

7. Transfers outside the UK

Some third parties that we share personal data with may be located outside the UK.

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

- ensuring that there is an adequacy decision by the United Kingdom government, or
- using standard contracts approved by the Information Commissioner's Office.

You can get a copy of the standard contract by contacting us (see contact details in section 12).

8. 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, and when compared with a similar manual process.

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 10, "Your rights".

9. For 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 specific purposes. The personal data will subsequently be deleted or irreversibly anonymised.

When your relations with us have terminated, or when the business relationship with the customer, client or counterparty that you have a connection with has terminated, we normally keep your data for another 5 or 7 years. This is due primarily to our obligations under the Money Laundering Regulations and requirements from the Financial Conduct 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 applicable limitation period is 12 years, then we may keep your data for up to 12 years
- if required due to your connection with our customer, client, agent or counterparty
- if retention is required due to other regulatory requirements

We keep voice recordings for 15 months for general documentation purposes and if the voice recording relates to investments, we have a legal obligation to retain it for 5 years as required in the UK Markets in Financial Instruments Regulations.

Surveillance videos are deleted 30 days after they were made. In certain circumstances, and in connection with a specific case, the information 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

- contact us on our main telephone number (+44 20 7410 8000)
- contact your adviser directly if you have one

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. 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 the UK 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 of 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 by contacting us on our main telephone number (+44 20 7410 8000) or by contacting your adviser directly if you have one.

Rights related to automated decision-making
When we use automated decision making in our processes you will always be notified separately of our legal basis for this and your option to not be subject to the automated decision making in advance. Furthermore you will be informed of the logic used for the automated decision making and you will be given the opportunity to 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 data. 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 your personal data is inaccurate, you are entitled to have the personal data rectified. If 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 in relation to the purposes for which it was collected.

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

- For compliance with a legal obligation, for instance if we are obliged by law to hold your personal data for a certain period of time, for example according to anti-money laundering legislation. 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 personal data we have registered about you is incorrect or if you have objected to the use of the personal data, you may demand that we restrict the use of the personal data to storage until the correctness of the personal data can be verified or it can be checked whether our legitimate interests outweigh your interests.

If you are entitled to have the personal data we have about you erased, you may instead request us to restrict the use of the personal 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 personal data be restricted to storage.

Withdrawal of consent
Where consent is the legal basis for a specific processing activity, you may withdraw your consent at any 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 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. You also have the right to request that we transmit this data directly to another data controller.

11. Changes to this privacy notice

We are required to update this privacy notice on a regular basis. 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).

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 (+44 20 7410 8000). 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, 75 King William Street, London EC4N 7DT. You can also lodge a complaint with the UK Information Commissioner's Office (further details are available on www.ico.org.uk or by calling 0303 123 1113).