Data Privacy Notice: Corporates & Institutions

Effective from November 17th 2020

This data privacy notice aims to assist you in understanding how and why we use personal information and your rights in relation to it, and to assist us in meeting our obligations under the General Data Protection Regulation (GDPR).

Danske Bank

Who are we and how does this notice apply to you?

Danske Bank A/S is a financial institution that offers financial advice and services to its clients. Danske Bank is the data controller for the processing of personal data referred to in this notice.

In the course of our business, we register and use information including personal data about individuals who are connected with a corporate customer of ours. This privacy notice applies to you if you are such an individual. You could be an authorised signatory, a beneficial owner, a director, a corporate cardholder, a District user, an employee, a guarantor, a provider of security or a third party connected to our customer.

Danske Bank's contact details are as follows:

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

Danske Bank A/S
acting through its branch in Ireland,
3 Harbourmaster Place,
IFSC, Dublin 1.

1. What personal data do we process, register and use?

We typically process the following types of personal data:

- Personal details such as your name, country of residence and date of birth, and if legally required, your PPS number
- Proof of identity such as your passport, driver's licence and birth certificate
- Contact information, including your address, mobile telephone number, work telephone number and email address.
- Professional information such as your education, profession, occupation, knowledge and experience
- Details about the services and products we provide including accounts, and corporate cards and access rights
- Details about how you use our services and products and your preferences in relation to them
- Digital information in relation to the 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 certain technical information including the type of device you use and the operating system
- Information provided by you in respect of your preferences or attendance at customer events
- Information about your visits to our offices, including video surveillance and CCTV footage
- Information provided by you by email or other electronic media in your engagements with us
- Information you provide during telephone conversations with us, including the call transmission itself.

2. What do we process, register and use your personal data for?

We 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 talk to them about products and services offered by Danske Bank, and, if they wish to avail of our services and products and to become a customer, for onboarding purposes in relation to identification and verification for anti-money laundering purposes.
- To comply with applicable law and regulation including identification and verification requirements under anti- money laundering legislation. In relation to anti-money laundering requirements, it should be noted that identification data is collected at regular intervals during our corporate customer's relationship with us, as required by law.
- To provide customer service and customer relationship management, including providing advice, administration, management of

employee corporate cards, management of District users, and handling of complaints.

- For prevention and detection of money laundering, fraud, and other types of financial crime.

- To improve, develop and manage our products and services and the way in which we set fees and process for our products and services, including using data analytics and statistics to improve products and services and to test our systems.

- To market our services and products, including marketing on behalf of other entities of the Danske Bank Group, only where we have your specific permission to do this or such marketing is otherwise permitted by law. We use cookies and similar technology on our website, including for marketing via digital channels. Please refer to our cookie policy for further information.

- For security, including the use of video surveillance and CCTV at the entrance to our branch, reception and customer areas.

- Where the personal data we hold is a mobile telephone number for an individual connected to a corporate customer, our purposes for processing include:

  (i) anti-payment fraud measures (for example, where we may need to verify the identity of individuals authorising a payment),

  (ii) to send a one-time activation code for the activation of an eSafeID device to satisfy our Strong Customer Authentication (SCA) obligations under PSDII in respect of District log-on flow (where this is not provided, it will be necessary for us to use additional factors to satisfy our SCA obligations such as requiring a visit to our offices in person), and

  (iii) for sending a one-time passcode for verification of e-commerce transactions to satisfy our PSDII SCA obligations in respect of e-commerce transactions (where this is not provided, it will not be possible for a corporate cardholder to complete ecommerce transactions after 1 January 2021.)

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

We will only register and process your personal data if we have a legal basis or "reason" to do so. This means that we register and use personal data when:

- you have granted us consent to use your personal data for a specific purpose, cf. GDPR art. 6.1(a)

- so that we can perform a contract with you e.g. as corporate cardholder cf. GDPR art. 6.1(b)

- we have to comply with certain legal obligations, cf. GDPR art. 6.1 (c), including:

  Obligations arising under:

  - Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

  - Taxes Consolidation Act, 1997

- Credit Reporting Act 2013
- European Union (Markets in Financial Instruments) Regulations 2017
- Consumer Protection Code 2012
- FATCA/CRS

or any amendment or replacement of this law which may arise.

Obligations to comply with:

- Court orders arising in civil or criminal court proceedings
- Binding requests from regulatory bodies such as the Central Bank of Ireland
- Binding search warrants, productions orders and other orders requiring the bank to provide assistance in civil or criminal matters

- we or the business or corporate customer that you have a connection with are pursuing a legitimate interest. This could be where we or the customer have a business or commercial reason to use your personal data, such as administering the services and products that the customer has requested, or giving you the necessary access to digital services, where we need to prevent or minimise the risk of potential fraud, where we need to prevent abuse of our systems, the law or regulation, where we need to prevent financial loss, or where we need to strengthen IT and payment security. We will only do so if our interest clearly outweighs your interest in not having your personal data processed by us, cf. GDPR art. 6.1(f).

4. What sensitive personal data do we process, register and use?

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

In particular, we may process information about:

- your religious or philosophical beliefs, or political opinions which may be identified during PEP and sanctions screening
- biometric data such as images we receive through CCTV footage and video surveillance
- your health e.g. food allergies if you are attending a client event with us

5. What do we process, register and use your sensitive personal data for?

We process sensitive personal data only when we need to, including for the following reasons:

- to comply with legal obligations that apply to us as a financial institution, such as. screening andidentification and verification
- for the prevention and detection of money laundering and other types of crime, including for fraud prevention and detection purposes
- to ensure the security of our premises

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

We may process sensitive personal data about you on the legal basis of:

- your explicit consent, cf. the GDPR art. 9.2(a)
- the establishment, exercise or defence of legal claims, cf. the GDPR art. 9.2(f)
- the processing relates to personal data which is manifestly made public cf. the GDPR art. 9.2(e)
- substantial public interest, cf. the GDPR, art. 9.2(g)

7. From where 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 corporate 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
- communicate with us via letter and digital means, including e-mails, or social media
- call us (or when we call we call you at your request) or to follow up on an inquiry from you and we record your call to meet a legal obligation, or when we have carried out a balanced assessment that it is in our legitimate interest to do so e.g. for the detection or prevention of fraud. If we are talking to you about investment services, we are legally required to record and store our telephone conversation. We will advise you on or before the call that the call is being recorded.

Personal data collected from third parties

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

- The corporate customer with whom you have a connection
- Shops, banks and payment and service providers when you use your corporate credit or payment cards, District or other payment services. We process the data to execute payments and prepare account statements, payment summaries and the like.
- Asset managers when we provide trade reports to their customers.
- the Central Office of the High Court, the Companies Registration Office and other publicly accessible sources and registers. We register and use the data they have about you to check that the data you have provided to us is accurate and to carry out PEP and sanctions screening.
- Credit rating agencies and warning registers. We process the data to perform credit assessments. We update the data regularly.
- Other entities within the Danske Bank Group, including branches and subsidiaries.

We use the data as permitted or required by law, for example to comply with group-based management, control and/or reporting requirements, to comply with anti-money laundering legislation and to provide all aspects of our products and services to the corporate customer with whom you have a connection

- External business partners (including correspondent banks and other banks) if permitted under existing legislation, for example to enable our customers to use banking services abroad, or to prevent and detect money laundering, fraud, abuse and loss

- the Central Credit Register in accordance with our obligations under the Credit Reporting Act 2013.

8. With whom do we share the information we have about you?

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 in the Danske Bank Group in order to provide you with all aspects of a product or service we are providing to the corporate customer with which you are connected, or to seek approval to do so e.g. in order to obtain credit approval for a loan

- Other entities in 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.

- Service providers authorised as an account information service, payment initiation service or card-based payment instrument providers, when the service provider requests information about the account belonging to the corporate customer with which you are connected.

- Public authorities and regulatory bodies as required by law or upon their request, including to an Garda Síochána and Revenue Commissioners under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (and any replacement or amendment thereof), to the Revenue Commissioners in accordance with the Taxes Consolidation Act 1997 and other tax legislation, to the Central Bank of Ireland to comply with our obligations under the Credit Reporting Act 2013 and other law and for statistical and other purposes, to the courts, to the Data Protection Commission, to the Financial Services and Pensions Ombudsman, to the Credit Review Office, to the Criminal Assets Bureau, to US, EU and other designated authorities in connection with combating financial and other serious crime, and to fraud prevention agencies.

- External business partners (including correspondent banks and other banks), for example, to prevent and detect money laundering, fraud, abuse and loss.

- Guarantors, individuals holding a power of attorney, the lawyers advising you or the corporate body with which you are connected, the accountants advising you or the corporate body with which you are

connected, and others you have authorised us to share the information with.

- Our external advisors, including our lawyers, accountants and auditors.
- Our suppliers, including 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.
- Third party providers such as platform providers and forensic providers who are assisting us with providing information to a regulatory body or other public authority.
- In connection with IT development, hosting and support, and to provide all aspects of the services and products we give to you, we transfer personal data to data processors, including data processors in third countries outside the EU and the EEA – see "Transfers outside the EU and the EEA and international organisations" below
- For social and economic research or statistics purposes, where it is in the public interest.

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

Some third parties with whom we share personal data may be located outside the EU or the EEA, such as Danske Bank UK or Danske Bank India. When Danske Bank transfers your personal data to third parties outside the EU and the EEA, we ensure that your rights are safeguarded and protected in such data transfers by:

- ensuring there is an adequacy decision
- using standard contracts approved by the European Commission or the Data Protection Commission in Ireland.

A copy of the EU model clause agreement used to document such arrangements may be obtained by submitting a request to our Data Protection Officer using the contact details below.

10. Profiling and automated decisions

Profiling is a form of automated processing of 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.

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

In Danske Bank Ireland, Corporates & Institutions we never use profiling or automated decisions to approve loans and credit products for our corporate customers.

In relation to the prevention and detection of money laundering, and in relation to the prevention and detection of fraud, we may use profiling and automated decision making in the checks we perform e.g. in protecting our customers against criminal or fraudulent activity we monitor transactions to and from accounts

and identify unusual transactions (for example, payments you, if you are a corporate cardholder, 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 12, "Your rights".

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

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

In accordance with the law (for example, the European Union (Markets in Financial Instruments) Regulations 2017), we may store data, documents and records for a period of seven years after the termination of the business relationship or the execution of a specific transaction.

12. Your rights

You have rights in relation to your personal data. See below for more information on how to contact Danske Bank about data protection and to exercise your rights.

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 personal data and about who receives your personal data, to the extent that we disclose data in Ireland and abroad. Your right of access may, however, be restricted by the law, to protect another's privacy , due to the prevention, investigation, detection or prosecution of criminal offences, due to the prevention of threat to our employees or due to business secrecy.

Rights related to automated decision-making
You can obtain information on how an automated decision affecting you 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 our processing of your personal information including when we rely on our legitimate interest to process your personal information. You also have the right to object to our use of your personal information for marketing purposes, including profiling that is related to such purpose.

Right to rectification of your data
If the personal data we hold about you is incorrect or inaccurate you are entitled to have the data rectified. If the personal 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 be 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, such as under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

- 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 your data 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
If the basis on which we are processing your personal data is the fact that you have consented to us doing so, you can withdraw consent at any point in time. Please note that if you withdraw your consent, we may not be able to offer specific services or products to the corporate customer with which you are connected. Please also note that we will continue to use your personal data if we have another legal basis or "reason" for holding it i.e. if we are required to do so by law.

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

13. Changes to this data privacy notice
We change and update this privacy notice on a regular basis. In the event of a change, the "effective from" date at the top of this data privacy notice 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 through our online banking channel District, to allow you to exercise your rights.

14. Contact details and how you can complain
You are always welcome to contact us if you have questions or concerns about your privacy rights and how we register, use and process personal data. You can contact our Data Protection Officer by writing to the:
Data Protection Officer, Ronan Coyle, Holmens Kanal 2-12, 1092 København K, e-mail: dpofunction@danskebank.com.

If you are dissatisfied with how we register and use 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 by writing to the **Data Protection Information Contact** and the **Legal Team (C&I)**, both at **Danske Bank, 3 Harbourmaster Place, IFSC, Dublin 1.**

You can also lodge a complaint with the **Data Protection Commission:**
Canal House, Station Road, Portarlington,
R32 AP23 Co. Laois,
email: info@dataprotection.ie
phone: +353 (0)57 868 4800 or
+353 (0)761 104 800.