Danske Bank International privacy notice

Effective from 25 November 2020

1. Introduction

This privacy notice applies to the processing of personal data by Danske Bank International S.A. (DBI) in Luxembourg. DBI is the data controller for the processing of the personal data described in this privacy notice.

Contact details: Danske Bank International S.A. 13, rue Edward Steichen, BP 173, L–2011 Luxembourg.

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.

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

2. What personal data do we process?

Depending on the services and products you have ordered or are interested in, we process different kinds of personal data, including

- personal details 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
- financial information, including details about your income, assets, debt, credit rating and insurance policies
- collateral, including market value, energy data and environmental aspects
- information about your education, profession, work knowledge and experience
- information about your family and household
- data on the environmental, social and governance (ESG) impact of your business where you are a sole trader,
- details about the services and products we provide to you, including accounts, cards, loans, credits, etc.
- 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 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 offices, including video surveillance, if any
- 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.

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 inform us of any changes.

3. What we use your personal data for

We process data about you to provide the best advice and solutions, protect you against fraud and fulfil our agreements with you.

We process personal data to provide you with the financial services or products that have been requested, including

- payment services
- accounts
- card services
- loans and credit facilities
- 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 on-boarding purposes in relation to identification and verification for anti-money laundering purposes.
- Customer services and customer relationship management, including advice, administration, credit assessment, 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 and/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. We refer to our cookie policy for further information https://danskebank.lu/privacy-statement-and-use-of-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 customer relationship with us as required by law.
- Security and crime prevention, including the use of video surveillance of the front of buildings, entrances to our premises, reception and customer areas, ATMs and counters.

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 Anti-Money Laundering Act (*Law of 12 November 2004 as amended*)
  - the Central Electronic Data Retrieval Act) (*Law of 25 March 2020 establishing a central electronic data system for IBAN accounts and safe-deposits boxes*)
  - Law of 25 November 2014 applying a/o mutual assistance and administrative cooperation between tax authorities in the EU
  - the FATCA Act of 24 July 2015
  - Law of 18 December 2015 on automatic exchange of account data for fiscal purposes CRS
  - the Financial Sector Act (*Law of 5 April 1993 as amended*)
  - the PSD2 Act (*Law of 20 July 2018 on the 2nd Payment Service Directive (EU)*)
  - the Data Protection Act of 1 August 2018
  - the MiFID Act (*Law of 30 March 2018 on markets in financial instruments as amended*)
  - the SRD II Act of 1 August 2019 (*implementing the 2nd Shareholder Rights Directive*)
- It is necessary to pursue a legitimate interest of DBI, cf. the 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 will do so only if our legitimate

interest in each case is not outweighed by your interests or rights and freedoms.

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 the following types of sensitive personal data:

- Trade union membership information
- Information about your health and your genetic background, for example inherited health qualities
- Biometric data, for example via facial recognition technology
- Information about your religious or philosophical beliefs
- Information about your political opinions

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
- for the purpose of giving you discounts negotiated with our partners or other external organisations
- 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, cf. the GDPR, art. 6.1(a) and 9.2(a)
- the establishment, exercise or defence of legal claims, cf. the GDPR, art 6.1(f) and 9.2(f)
- 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 example with your adviser
- 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

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 for documentation and security purposes. Before an employee answers a call or before you enter the queue, you will be notified if the call will be recorded. In a few situations, for example in case of a long waiting time, your call may be redirected to a non-recorded employee without notification to 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 service 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.
- Publicly accessible sources and registers. We process the data, for example for identification and verification purposes and to check data accuracy.
- 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 Financial Intelligence Unit and the Financial Supervisory Authority in Luxembourg 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 with whom you have a connection.

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 the Financial Intelligence Unit and the Financial Supervisory Authority in Luxembourg 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 authorised as an account information service, payment initiation service or card-based payment instrument provider, if you (or someone who via our online services can view information about your accounts or initiate payments on your behalf) request such a service provider to receive information about you.
- Guarantors, 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(s).
- 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 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 shipment.
- 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 Financial Intelligence Unit and the Financial Supervisory Authority in Luxembourg in accordance with the anti-money laundering legislation and tax authorities in accordance with the legislation in Luxembourg, incl. e.g. statistical and other purposes.
- Regulators, such as the Financial Supervisory Authority in Luxembourg (CSSF), law enforcement agencies and authorities in Luxembourg and other countries, including countries outside the EU and the EEA, in connection with their duties.
- Credit rating agencies. If you default on your obligations to DBI, we may report you to credit rating agencies and/or warning registers in accordance with applicable law.
- If you activate the payment information function in your smart phone, it is 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 in Australia, Canada and India.

When the Danske Bank Group 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 safeguards by

- 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 and value assets and for marketing purposes. If you are a sole trader, we use profiling and data modelling to assess the environmental, social and governance (ESG) risk of your business.

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 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 determine 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 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, "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 registered and used.

When your business relations with us have terminated, we normally keep your data for another ten years. This is due primarily to our obligations according Luxembourg law, incl. the Commercial Code and the Anti-Money Laundering Act as well as requirements from the Financial Supervisory Authority in Luxembourg. 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 other regulatory requirements

If you, as a potential customer, have asked for an offer for a loan or another product or service, but refuse the offer and do not become a customer, your personal data will normally be stored for six months, but may for some purposes be stored longer to comply with other legal obligations, for example under the Anti-Money Laundering Act.

11. 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 (+352 4612751)
- contact your Private Banker directly

See section 13 for more information on how to contact DBI 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 Luxembourg 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.

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 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 the Commercial Code. 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. Use will be restricted to storage only 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 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. 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 a 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 (+352 4612751. You are also welcome to contact your Private Banker directly.

You can contact the Danske Bank Group's Data Protection Officer by email at 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:

Danske Bank International
Legal Department
BP173
L - 2011 Luxembourg
E-mail: r4538leg@danskebank.lu

You can also lodge a complaint with CNPD (Luxembourg's data protection agency) through www.cnpd.lu.