Danske Bank A/S Privacy Notice for Business Customers (Poland)

Effective from 1 November 2024

1. Our role as data controller and the reason for this privacy notice

This privacy notice applies to the processing of personal data of individuals who relate to business customers of Danske Bank A/S, including large corporates or institutions. You may as example be an authorized signatory, a beneficial owner, a director, an employee, a guarantor, a pledgor or another third party who relates to a business customer. In any of these relationships, Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark (CVR 61126228), acting through Danske Bank A/S S.A. Branch in Poland, Wspólna str. 70, 00-687 Warsaw, Poland (Danske Bank), processes your personal data acting as a data controller.

Danske Bank has appointed a Data Protection Officer (DPO), the contact details of which are –

DPO of Danske Bank A/S,

Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark

Email addressn – dpofunction@danskebank.dk

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

2. Types of personal data we collect and process

Depending on your relations with our business customer and Danske Bank, we process different types of personal data, including but not limited to the personal data set out below

- Identification information, such as – your name/names, surnames, social security number or other national ID number (including – tax identification number (NIP), statistical number (PESEL), ID number) and proof of identity document such as a copy of your passport (including details such as – passport number, issuance date of passport, expiry date of passport), ID Card (including such details as – issuance date of ID, expiry date of ID, country of ID issuance), driver's license and/or birth certificate, signature, citizenship, date of birth, place of birth, country of birth, mother's maiden surname
- Contact information, including your address (private address and business address), address of permanent residence, address of correspondence, telephone number (private/business) and email address (private/business)
- Details about the services and products we provide to you or our customer including accounts, cards and access rights
- Information related to your usage of our websites, platforms, and digital applications, including – To the extent applicable and necessary traffic, location, tracking and communication data, e.g., collected by use of cookies and similar technology, Cookie policy (danskeci.com). Information about your devices used to access our websites as well as technical information, including the type of device and operative systems
- 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 of online meetings with you

- Other personal data as necessary to provide you or our business customer with specific products or services, or if we are required by law to do so (for example – mother's maiden surname

Our ability to offer the best possible advice and solutions for you and our business customer very much depends on how well we know you and our customer, and consequently, it is important that the information you provide is correct and accurate and that you inform us of any changes.

3. Why & on which legal basis we process your personal information

Generally, we process personal data about you to provide you or our business customer with the services and products chosen, to offer you or our customer the best advice and solutions, to protect our business customer, you and Danske Bank against fraud, to fulfil our agreements with you or our business customer, and to comply with applicable regulations, including data security and data protection requirements.

Below, we have listed some examples on why and which legal basis we use, when we process your personal data in various contexts

- When we onboard you as a user of an online product or platform for our business customer, 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*, cf. GDPR art. 6.1(c), for example, pursuant to the Polish Anti-Money Laundering and Counteracting of Terrorism Act (**Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu**)
- When we conclude a contract with business customer and you as a representative acting on behalf of our business customer, we process your personal data for both identification, verification purposes and obligation arising from Polish Civil Law and Banking Law. The legal basis for this processing is to comply with a legal obligation*, cf. GDPR art. 6.1(c), for example, pursuant to the Banking Law and Civil Code (**Ustawa prawo bankowe, Kodeks Cywilny**)
- When we provide our business customer with a financial product you have requested or consider to obtain on behalf of our business customer (such as payment services, accounts, card services, loans, credit facilities, digital banking solutions, investment services, financial advice, insurance, 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 authorized to request information about you or our customer) we do this because you or our business customer have entered or consider entering into an agreement with us on delivery of a service or product, cf. GDPR art. 6.1(b) and to pursue legitimate interests, cf. GDPR art. 6.1(f)
- Sometimes we share your personal data with another company within the 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 business customer, cf. GDPR art. 6.1(b) and in relation to the transfer of your personal data we pursue legitimate interests to use and share your personal data for such specific purposes yourself, cf. GDPR art. 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 fulfill a contract with you, cf. GDPR art. 6.1, (b), or subject to a legal obligation*, cf. GDPR art. 6.1(c), or to pursue a legitimate interest, cf. GDPR art. 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, cf. GDPR art. 6.1(c), cf. GDPR art. 32, or we may pursue a legitimate interest, cf. GDPR, art. 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, cf. GDPR art. 6.1 (b) so you on behalf of our business customer may receive a price quotation or a product offering and in relation to processing your personal data we pursue a legitimate interest, cf. GDPR, art. 6.1(f)
- When we carry out fraud detection on card and account transactions, including processing of behavioral 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*, cf. GDPR art. 6.1(c), and to pursue legitimate interests, cf. GDPR art. 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, cf. the cookie requirements for collection of data and GDPR, art. 6.1(a) for the subsequent use of data. We refer to our cookie policy for further information 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*, cf. GDPR art. 6.1(c) and to pursue legitimate interests of Danske Bank, cf. GDPR art. 6.1(f)
- We process your personal data for security reasons, for instance various loggings, cf. GDPR art. 6.1(c) and art. 32. We use video surveillance and record such of the front of buildings, entrances to our branches and other premises, reception and customer areas
- 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, cf. GDPR art. 6.1(b). We may also invite you to events and send you invitations to maintain proper business relations in areas, which we think may have your interest
- 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, cf. GDPR art. 6.1(c)

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

- The EU Markets in Financial Instruments Regulation (MiFIR)
- The EU Regulation on Market Abuse (the Market Abuse Regulation)
- The EU Markets in Financial Instruments Directives (MiFID I and II)
- The General Data Protection Regulation (GDPR)
- The Polish Data Protection Act
- The Polish Accounting Act
- The Polish Civil Code
- The Polish Banking Law
- The Polish AML Act
- The Polish Financial Information System Act
- The Polish Tax Ordinance
- The Polish Trading on Financial Instruments Act
- The Polish Payment Services Act
- The Polish Regulation of the Minister of Finance on specific accounting principles for banks
- The Polish Regulation on the procedure and conditions of conduct of investment firms, banks referred to in Art. 70 sec. 2 of the Act on Trading in Financial Instruments, and custodian banks
- The Polish Regulation on detailed technical and organizational conditions for investment firms, banks referred to in Art. 70 sec. 2 of the Act on Trading in Financial Instruments, and of custodian banks

- Regulation of the Minister of Internal Affairs and Administration of September 7, 2010, on the requirements to be met by the protection of monetary values stored and transported by entrepreneurs and other organizational units

4. How we collect the personal data we have about you

Personal data collected from you

We collect information, you share with us or from 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, for example with your advisors
- Talk to us on the phone
- Use our website, mobile applications, products, and services
- Participate in our customer surveys or promotions organized by us
- Communicate with us via letter and digital means, including e-mails, or on social media
- Use our digital solutions and apps or visit our websites
- Leave personal data which we might collect from electronic communication, telephone and video recording and monitoring
- Participate in hospitality events organized or hosted by us
- Subscribe to our newsletters

We are obliged to monitor and store all electronic communications related to investment services, for instance when we chat, email or speak on the phone with you according to the EU Markets in Financial Instruments Directives and Regulations (MiFID I and II, MIFIR) and also according to the Polish Banking Law, the Polish Trading on Financial Instruments Act, and few others acts related to investment firms and banks. We also store video recordings of you if you have visited our premises. We store this information according to the requirement in Polish Labor Code and Regulation of the Minister of Internal Affairs and Administration of September 7, 2010, on the requirements to be met by the protection of monetary values stored and transported by entrepreneurs and other organizational units.

Incoming and outgoing calls and online meetings are recorded, listened to and stored to comply with regulatory requirements but also for documentation purposes. We refer to our information on recording of phone conversations for details on our recording and processing of personal data in relation to voice and online meeting recordings Recording of phone conversations | Danske Bank.

Personal data collected from use of cookies

We may 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 necessary cookies to enable you to use our services. If you consent to additional cookies, such as functional, statistical and/or marketing cookies, we set cookies according to your consent to measure, analyze and improve use and performance of our products and services and to the extent applicable.

Some of the marketing cookies are owned by third parties, such as Meta Platforms Inc. or Alphabet Inc. 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. We refer to our cookie policy Cookie policy (danskeci.com) for further information.

Personal data we collect from third parties

We receive and collect personal data from third parties, including for example from

Our business customer to which you have a relationship

Shops, banks, payment and service providers when you use your credit or payment cards or other payment services. We process the personal data to execute payments and prepare account statements, payment summaries and the like

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 such as the Capital Requirement Regulation (CRR)

External data controllers such as business partners (including correspondent banks and other banks), and vendors, if permitted under existing legislation, for example to provide you or our business customer 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.

5. Third parties that we share your personal data with

We will keep your information confidential under applicable banking secrecy rules, however, we may disclose and share necessary personal data with companies form Danske Bank Group and third parties where we have an appropriate legal basis as per some of the examples set out below, who are also obliged to keep your personal data confidential

- Other entities of the Danske Bank Group, for example to provide you with better customized 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 or risk management requirements imposed by law or regulations (e.g., Capital Requirement Regulation) and/or reporting requirements established by law or required by regulators
- The respective public authorities (such as – General Inspectorate for Financial Information, Financial Supervision Authority, National Tax Administration, Police and Public Prosecution as well as other relevant investigation authorities such as Internal Security Agency, Central Investigation Office, etc.) in accordance with anti-money laundering legislation
- If you have asked us to transfer money to others, we disclose personal data about you that is necessary to identify you and to perform the transaction
- When we process international payments, your personal data may be processed by Swift in the context of the Swift's Transaction Processing Services, which enable us to send and receive financial messages or files, and to pre-validate, track, and manage financial transactions. For further information on the data protection practices of Swift in relation to the processing of your personal data in the context of the Swift Transaction Processing Services, please consult Swift´s Privacy Statement for further information Privacy Statement | Swift
- Service providers authorized as an account information service, payment initiation service or card-based payment instrument provider, if you (or someone who via our online services can view information about your accounts or initiate payments on your behalf) request such a service provider to receive information about you
- Card producers, when cards are imprinted with your personal data
- Card issuers, payees, and holders of lists of blocked cards, e.g., Fiserv, Nets, in case you request us to block your debit or credit card, or if we have reasonable suspicion of card abuse or for card operators to be able to prevent fraud

- Guarantors, individuals holding a power of attorney, lawyers, accountants, or others you or our business customer have authorized us to share information with
- If you have joint financial products with someone, such as a joint account or child savings account, we share your information, including personal identification number, with your co-product holder/owner and tax reporting
- Cards operators, payment services providers and other banks if required or permitted under existing legislation, to prevent and detect money laundering, fraud, card abuse and loss
- Lawyers, accountants, consultants related to the Danske Bank Group
- 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
- IT service and outsourcing providers as well as personal data processors to provide services to us and you
- 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 Polish Police, Polish Public Prosecutor, the Polish tax authorities in accordance with the Polish Tax Law, social services and the Polish National Bank
- Regulators, such as the Polish Financial Supervisory Authority (**Urząd Komisji Nadzoru Finansowego**), Data Protection Agency (**Prezes Urzędu Ochrony Danych Osobwych**), and law enforcement agencies and authorities in Poland or abroad, in connection with their duties
- For social and economic research or statistics purposes, including where it would be in the public interest
- In connection with transactions (including transfers, asset sales, mergers and acquisitions) which entails transfer of the whole or part of our business to another company, we may share your personal data to the extent necessary to complete the transfer and your customer relationship within the framework of the legal requirements we need to comply with

6. *Transfer of personal data to third countries*

Your personal data may be processed by our business partners within EU/EEA in connection with our request to provide you with various services on our behalf.

In some cases, we use various IT-suppliers, business partners, and consultants, etc., who can access personal data from countries outside EU/EEA ('third countries'), if necessary, despite such personal data generally not being stored in these third countries. Such IT-providers, partners, etc. are subject to data processing or data sharing agreements with us, which ensure that they process personal data only in accordance with the GDPR and applicable EU national data protection laws.

We primarily choose providers/partners who process personal data within EU/EEA, and secondly suppliers in countries that appear on the EU Commission's list of safe third countries and only, if necessary, suppliers in other third countries. Accordingly, we rely on different legal bases depending on the country of the personal data receiver

- If we transfer your personal data to parties in countries where the European Commission has found that the country ensures an adequate level of protection, we rely on the adequacy decision of the European Commission as our GDPR art. 45 transfer basis
- If we transfer your personal data to parties located in the USA, we may rely on the EU-US Data Privacy Framework to certified parties as our GDPR art. 45 transfer basis
- If we transfer your personal data to other third countries, we may rely on the European Commission's standard contractual clauses (also known as SCCs) or business partner's binding corporate rules (also known as BCRs) together with implementation of adequate supplementary measures or carry out a review of local legislation to ensure that your personal data receives an essentially equivalent level of protection to that guaranteed in the EU/EEA, if and where deemed necessary as our legal basis for transfer under GDPR art. 46

- We may also transfer your personal data to parties outside EU/EEA based on the specific exemptions set out GDPR art. 49, in example GDPR art. 49, no 1, litra e) if the transfer is necessary for our establishment, exercise or defense of a legal claim

When transferring personal data to a business partner outside of the EU/EEA, we ensure that our transfer of your personal data is conducted in accordance with GDPR Chapter V.

7. Profiling and automated decisions

Profiling

We are constantly working to develop, improve and manage our products and systems. We use data analysis, statistics and evaluate our analyses, models and theories on customer behaviour with use of advanced analytical innovative methods, such as machine learning and AI. This helps us i.e.to set fees and prices, provide the basis for our marketing and business development. We continually process customer personal data, develop profiles by use of machine learning models to help us to offer products that meet our customer's unique needs and prioritise customer enquiries in an efficient way. We also process personal data for process and system development and improvement, including through tests.
We use cookies and similar technology on our websites and in our digital apps, for marketing purposes, including for marketing via digital channels and social platforms. You can read more about this in our cookie policy.

Automated decision-making

With automated decision-making, we use our systems to make decisions without any human involvement based on the personal data we have about you. Depending on the specific decision, we also use personal information from public registers and other public sources. Automated decision-making helps us ensure that decisions are quicker and more fair, efficient and correct than decisions made through a similar manual process.

See section 10 'Your rights' for more information on your rights in relation to automated decisions.

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 stated by the legislator. The personal data will subsequently be deleted or irreversibly anonymized.

We have many different processes where we use your personal data and many different legal bases for retention of your personal data. Our retention criteria and retention periods vary from a few minutes up to 12 years. Below you see some examples of retention periods, but please note that the list is not meant to be exhaustive

- We keep your account information for up to 10 years due to the statutory limitation period
- We keep your Know Your Customer information for as long as our business customer is a customer and for additional 5 years as required in the Polish Anti-Money Laundering and counteracting of terrorism Act
- We keep credit and collateral agreements for up to 12 years after expiry to document our agreement so we may defend our legal rights within the statutory limitation period
- We keep your consent to our use of cookies for one year unless you withdraw it earlier
- We keep your voice recordings for a legal obligation to retain it for 5 years required in MiFID I and II, up to 7 years on request of the regulator. Reference is made to our information on recording of phone conversations for details on our recording and processing of personal data in relation to voice and online meeting recordings **Recording of phone conversations | Danske Bank**
- Surveillance videos are deleted 30 days after they were made. In case of a police investigation, the video may be stored for a longer period

8. Your rights

Your rights in relation to personal data are described below. To exercise your rights, you can use all channels to contact us. Examples on ways to contact us could be

- Contact us on our main telephone number (+45 70 12 34 56)
- You can contact our Group Data Protection Officer by email at – dpofunction@danskebank.com.

See section 10 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. 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 can 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.

If you wish to exercise your right to insight under GDPR the best way to contact us will be for instance to write to GDPR-insight@danskebank.dk, however you may also contact us via your adviser or via message in District, eBanking or Mobile Bank.

Rights related to automated decision-making

When we use automated decision making in our processes you will always be notified separately on our legal basis for this and your option to not to be subject to the automated decision making in advance. Furthermore, you will be informed on the logic used for the automated decision making and you will be given the opportunity to express your point of view and to object to the decision, and of your right to request a manual review of any automated decision.

Right to object to processing

In certain circumstances, you have the right to object to the processing of your personal data, for instance when we use automatic decisioning processes, or for example, when the processing is based on our legitimate interests.

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

Right to rectification of your data

If your personal data is inaccurate, not up-dated, you are entitled to have your personal data rectified. If your 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 for the purposes for which it was collected.

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

- To comply with a legal obligation, for instance if we are obliged by law to hold your personal data for a certain period, for example according to the Polish Anti-Money Laundering Act or the Polish Accounting Act. In such situations, we cannot erase your personal data until the required retention period has expired

- For the performance of a task carried out in the public interest such as sending statistical data to the relevant authorities, as provided for in the applicable provisions of law (e.g., National Bank of Poland)
- For establishment, exercise, or defense 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 our use of the personal data, you are entitled to obtain restricted processing of your personal data for storage only until we can verify the correctness of the personal data or if our legitimate interests outweigh your interests or not

Data portability

Under specific circumstances, you have the right to receive personal data which you have provided to us yourself in a structured, commonly used, and machine-readable format for personal use. You also have the right to request that we transmit this data directly to another data controller.

9. Changes to this privacy notice

We are required to update this privacy notice on a regular basis. When we do, you will see, that the 'effective from' date at the top of this document changes. 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).

10. 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 (+45 70 12 34 56) or contact the business customer adviser directly in District, eBanking or Mobile Bank or you can send us a letter to Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark.

You can contact our Data Protection Officer with all questions on our use of your personal data by email to dpofunction@danskebank.com or by sending a letter to the above address.

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 also lodge a complaint with the Polish or Danish Data Protection Authority – The President of the Personal Data Protection Office in Poland (Prezes Urzędu Ochrony Danych Osobwych) – If you believe that the processing of your personal data violates the law at – Stawki 2 str., 00-193 Warszawa.

If, for example, your residence or the place of the alleged infringement is in or is related to another member state than Denmark or Poland, you can typically also lodge a complaint with the Data Protection Authority in that member state. You always have the option to try your case in court.