How we use your Personal and Business Information

Correct as at - 17 December 2024

To read this on our website, you can visit our dedicated Privacy Notice page.

Data Protection Privacy Notice

This notice explains how we collect, create, use, share, store and delete your personal and business information. It sets out your rights under UK data protection law and regulation.

We are required to update this notice from time to time. If any changes significantly affect you, we'll let you know so you can exercise your rights.

This privacy notice applies to:

- **Customers –** Anyone who has accounts or uses our banking services
- **Former Customers –** Anyone who used to have accounts or used our banking services
- **Prospective Customers –** Anyone who has enquired about or applied for banking services
- **Visitors –** anyone who visits our premises, websites, or contacts us in any way
- **Beneficiaries and Authorised Signatories –** Anyone associated with accounts, like those who have permission to sign on an account
- **Guarantors –** Anyone who guarantees loans or other financial products for customers
- **Third Parties –** Anyone whose information we get from customers, such as those appointed under a power of attorney

This notice applies to Danske Bank UK, the trading name of Northern Bank Limited, a member of the Danske Bank Group (the Group). Companies within the Group will also look after your personal information based on this privacy notice.

The Bank has appointed a Data Protection Officer (DPO) who you can reach at:

Data Protection Officer, Danske Bank, Donegall Square West, Belfast, BT1 6JS or by emailing us at yourprivacyrights@danskebank.co.uk.

Your Rights

Under the UK Data Protection Act you have certain rights regarding your personal information:

- **Right of Access** – You can ask if we process your personal information and request a copy
- **Right to Rectification** – If you believe the personal information we hold about you is inaccurate or incomplete, you can request us to fix it
- **Right to Erasure** – You can request us to delete your personal information. We will comply if no legal or regulatory reason requires us to keep it
- **Right to Restrict Processing** – You can ask us to stop temporarily or permanently processing your personal information. Please note that this may prevent us from providing an account or service
- **Right to Object to Processing** – You can object to processing of your personal information under certain circumstances
- **Right to Data Portability** – You can ask us to transfer your personal information to another party
- **Right to Withdraw Consent** – If you gave us consent to process your personal information, you can withdraw it at any time
- **Right to Object to Marketing** – You can ask us to stop processing your personal information for marketing purposes
- **Right Not to Be Subjected to Automated Decision-Making** – You can request human involvement in any decision that would have a legal effect on you

Exercising your rights is usually free and we typically comply within a month. However, this can be extended in certain circumstances.

More information on your rights can be found on the Information Commissioner's website, ico.org.uk/for-the-public/

To exercise any of your rights, write to our Data Protection Officer at Danske Bank, Donegall Square West, Belfast, BT1 6JS, or email us at yourprivacyrights@danskebank.co.uk.

Personal Information we collect

Depending on the services you use, or you are interested in, we will collect and process the minimum amount of personal information required to provide those products and services. This includes the following:

- **Personal Details** – Such as your name, addresses, residential status, education, employment, phone numbers, email addresses, and information used to verify your identity like photo ID (passport or driver's license)
- **Financial Information –** This includes your income, assets, debts, credit ratings, insurance policies, pensions, taxes, household details, and details of others you have a financial connection with or anyone you authorise to act on your behalf
- **Account Information** – Information on the accounts and services we provide, such as account numbers, cards, account balances, unique identifiers, account and contact preferences, transaction history, and payment details
- **Personal Preferences –** Information on how you use our services and your preferences in relation to these, including those in relation to marketing and cookies
- **Additional Support Information –** Details of any additional support agreed to help you operate your accounts and for when we communicate with you
- **Communications –** We keep records of communications between you and us, including issued documents, notes, emails, phone calls, digital chats, and meetings

- **Technical Information –** Unique identifiers such as type of device, IP addresses, device operating system, which you use when accessing our websites or banking applications
- **Biometric Data –** We temporarily retain photo IDs ('selfies') during some account opening processes, design our applications to make best use of biometrics on third-party devices, and on occasion use behavioural biometrics, such as typing patterns and movement data to enhance device security and provide better user experiences
- **Video Recording –** Images captured when you visit our premises and use our cash machines
- **Cookies –** We collect information from your device, or store information on your device in the form of cookies to enhance security, improve user experience, and remember your choices and preferences. You can find more details on our Cookie Policy on our website

Providing accurate information is essential to offering the best possible service. Please ensure the information you provide is correct and inform us of any changes as soon as possible.

How we collect your personal information

We may collect your personal information in several ways

Directly from you – This includes information you provide or that we gather by observing your actions, such as:

- Filling out application or other forms for our products or services
- Submitting specific documents to us
- Using your accounts
- Participating in appointments, such as with a mortgage advisor or broker
- Talking to us on the phone (please note, calls may be recorded for compliance and service improvement purposes, and you'll always be notified when recording is taking place)
- Using our website, mobile applications, products, and services

- Participating in customer surveys, promotions, or market research
- Communicating with us by letter, digitally or on social media

From the use of cookies

We use cookies and similar technologies on our websites and apps. Necessary cookies are set automatically, while functional, statistical, and marketing cookies are set only on your consent. Some marketing cookies are owned by third parties, such as Meta or Google, and we share responsibility for the use of your personal information. Visit our Cookie Policy on our website for more details.

From third parties – This includes

- Shops, banks, and payment service providers when you use your cards or other payment services
- Others with whom you have a financial link, such as when assessing applications for joint accounts or loans
- Advisors and others authorised to act on your behalf
- Digital channels and social media platforms such as Facebook and LinkedIn
- Other Danske Bank Group entities, if we have your consent, or if legislation requires us to share and receive information
- External third parties, such as business partners and vendors, for providing banking services or to prevent fraud, abuse, and loss
- Credit reference and fraud prevention agencies used to verify your identity, accuracy of information provided, and manage your accounts, such as decisions on creditworthiness. Also used to prevent criminal activity, fraud, money laundering, and to trace and recover debts. Further details of the agencies used can be found on our details of credit reference agencies (PDF)

Why we collect and process your personal information

We collect and use your personal information for a variety of reasons for which the Bank must have a legal basis for any processing. We list some examples of why and on which legal basis we process your personal information:

- **To process applications –** We process your personal information for identification, verification, and anti-money laundering purposes when you apply for our services, which is completed under legal obligations.
- **To provide financial products –** We process your personal information when providing you with accounts, cards, payment services, loans and more. We undertake processing based on the contractual arrangement with you.
- **To manage your accounts –** This includes making payments, customer advice, administration, credit assessment, marketing, which are completed under legal obligations and in pursuing or legitimate interests.
- **Sharing information with third parties –** Whether a company within the Group or to a third party that provides you with a service, we do this where you have entered into a contractual agreement for a product or service and under our legitimate interests.
- **To communicate with you –** To send you information, such as statements and service updates. This is undertaken under our contractual arrangement with you and to comply with legal obligations.
- **To improve our IT-systems –** We may use personal information for analytics to evaluate our systems or models, ensuring accurate processing and effective security arrangements, based on our legal obligations and a legitimate interest.
- **When setting fees and interest rates –** We use data analytics and statistics, to set and communicate changes in fees and interest rates based on our contractual arrangement, legal obligations and to pursue our legitimate interests.
- **To prevent fraud –** We conduct fraud detection and prevention measures on card and account transactions, which may include behavioural information to identify unusual or suspicious use, which we do to comply with legal obligations and to pursue our legitimate interests.
- **For profiling and marketing –** We process your personal information when profiling and marketing our products and services, including any provided by Group companies, which we undertake based on your consent.

- **The use of cookies and similar technologies –** Which are used on our websites and within our digital applications, for which we rely on your consent.
- **To comply with policies and legal requirements –** We regularly assess, check, test, and monitor our compliance with internal policies and procedures to comply with legal obligations and pursue our legitimate interests.
- **For video surveillance –** We record images around and within our premises, cash machines, and at our counters to provide security for staff and customers, to comply with legal obligations and for our legitimate interests.
- **For building, maintaining, and testing models –** Relates to models that are required for credit risk exposures and internal ratings-based modelling for the assessment of capital requirements, undertaken to comply with legal obligations.
- **Other legal, regulatory, administrative and compliance activity –** Including identification and verification associated with anti-money laundering, risk management, and detection and prevention of fraud, credit fraud and other financial crimes, all based on legal obligation.
- **For sharing with Credit Reference Agencies (CRAs) –** We process your personal information to produce Credit Account Information Sharing (CAIS) data, which is shared with CRAs for creditworthiness assessments, risk management, fraud prevention, promoting responsible lending, and market protections, which we undertake to comply with legal obligations.

We will only process criminal convictions information

- Where used to comply with legal and regulatory obligations and to defend legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may collect and process sensitive personal information (also known as special category data) which can include information relating to health, racial or ethnic background, sexual life, biometric data, or legal proceedings. We only collect and process your sensitive personal information if any of the following is applicable:

- With your explicit written consent.
- Where we are permitted to do so by the law.
- If needed in the public interest.

Where the collection of sensitive personal information is undertaken based solely on your consent you have the right to remove that consent at any time. Although if you withdraw your consent, we might not be able to provide you with specific services or products.

For further information on 'lawful bases' used for data processing, you can refer to the ICO website.

Third parties that we share your personal information with

There are circumstances where we need to provide information to others to helps us manage your account, when it's in your interest, and/or when we're under a contractual, legal, or regulatory obligation. Examples of when we share personal information include:

- **Other parts of the Danske Bank Group –** We share personal information to provide you with the products and services you require and to comply with group-based management requirements
- **Local and national crime authorities –** The reporting of unusual activity that could indicate criminal or fraudulent activity as part of our legal obligations
- **Payment service providers –** We share personal information to facilitate payments you wish to make, including identity verification
- **Joint account holders –** Anyone with whom you hold a joint financial product will receive transactional information, which may include your personal information
- **Third party service providers –** We share personal information with third parties that provide all or parts of services. These parties are obliged to keep your personal information confidential
- **Card producers –** We share personal information to produce new or replacement cards
- **Third parties that you authorise –** This includes parties such as guarantors, those holding power of attorney, solicitors, accountants, or any other advisors you authorise us to share personal information with

- **Marketing Companies –** We share personal information with social media companies, such as Meta and Google when we hold consent for direct marketing
- **Regulators –** We share information with regulators, such as the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA) and the Information Commissioner's Office (ICO) to comply with regulatory requirements
- **Public authorities –** This could include organisations such as the Police Service of NI (PSNI), the Courts Service, National Crime Agency (NCA), Serious Fraud Office (SFO), or Social Security Agency (SSA) when they submit a formal request with legislative support
- **Credit Reference/Rating Agencies –** We share Credit Account Information Sharing (CAIS) data with agencies in accordance with contractual arrangements and other government agencies based on legal obligations
- **Debt Collection Agencies (DCAs) –** We share personal information if third party collection is required following a default of a credit agreement
- **Research and statistical purposes –** We may share your information where it is in the public interest

Transfer of personal data outside of the UK

Your personal information may be transferred outside of the UK and the European Economic Area (EEA), to allow third parties to provide services and process your information on our behalf.

In some cases, we use various IT-suppliers, business partners and consultants, etc., who can access personal information from countries outside of the UK/EEA, if necessary, despite such personal information generally not being stored in these third countries. All such providers are subject to data processing or data sharing agreements with Danske Bank, which ensure that any processing is in accordance with the General Data Protection Regulation (GDPR) and applicable national laws.

We primarily choose providers/partners that process personal information within the UK/EEA or those with recognised adequacy arrangements, and only, if

necessary, providers in other third countries. We rely on different legal bases depending on where the personal information is processed.

- In respect of the transfer of personal information within the EEA, which covers most personal information transferred within the Danske Bank Group. We rely on the EU-UK Trade and Cooperation Agreement (TCA) and the European Commission's adequacy decision when sharing personal information as ensures an equivalent level of protection as required by the UK General Data Protection Regulation (GDPR)
- If there are third countries outside of the UK/EEA that are covered by the European Commission's adequacy decisions, this allows for free flow of personal information to these countries
- For transfers between the USA, we may rely on the UK Extension to the EU-US Data Protection Framework to certified parties
- For the processing of your personal information to other third countries, we may rely on ICO approved binding corporate rules (BCRs) or the international data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses (SCCs) along with a document setting out adequate supplementary measures to ensure your personal information receives an equivalent level of protection to that guaranteed within the UK
- We may also transfer your personal information outside of the UK based on specific exemptions within Article 49(1)(e) of the UK GDPR in the context of defending legal claims

For all transfers outside the UK we ensure that our transfer of your personal information is conducted in accordance with the UK regulation. You can read more on personal information transfers to third countries on the ICO's website.

How long we keep your personal information

We keep your personal information for the duration it's needed for the original purpose, or as required by law. This means we typically keep most of your personal information for as long as you're a customer. After you stop being a customer, we continue to store your personal information for up to 7 years for the following reasons:

- **Complaints –** To respond to any complaint, or to demonstrate that we treated you fairly
- **Research –** To analyse personal information for research purposes
- **Regulatory Compliance –** To comply with legislative and regulatory requirements

If you are a potential customer and don't end up becoming a customer, any personal information you shared may be stored for up to 12 months, depending on the product or service you enquired about.

Once we no longer need to retain your personal information in a form that identifies you, we will permanently delete or destroy it or anonymise it in a way that ensures you identity is never recoverable.

Profiling and automated decision-making

Profiling refers to an automated process where we use your personal information to evaluate certain personal aspects relating to you, such as your economic situation, personal preferences, interests, reliability, behaviour, location, or movements.

We use profiling and data modelling to offer you specific products and services that align with your preferences. This includes assessing credit risk, prevent money laundering, detecting, and preventing fraud, evaluating the likelihood of default risk, and for marketing purposes.

Automated decision-making involves using automated processes, including profiling, and analysing your credit data from other lenders, to make decisions about you. For instance, we may use automated decision-making to approve applications, make credit decisions or preventing fraud during our business relationship with you.

We will always inform you when we use your personal information in an automated decision-making process. You have the right not to be subject to automated decision-making, if it affects your legal rights or has a significant impact on you, such as the refusal of an online credit application.

Use of Artificial Intelligence (AI)

We are continuously striving to enhance our services and improve your experience with us. As part of this effort, we may implement Artificial Intelligence (AI) technologies in the future.

If we decide to use AI technologies to process personal information, we will:

- **Purpose and scope –** Clearly define the specific purposes for which AI will be used, such as personalisation of services, data analysis, or automated decision-making
- **Data Security –** Implement robust security measures to protect your personal information from unauthorised access, misuse, or disclosure
- **User Rights –** Respect your rights regarding your personal information
- **Impact assessment –** Conduct regular assessments to understand the impact of AI on your privacy and take necessary steps to mitigate risks
- **Third-party involvement –** Ensure any third parties involved in the AI processing of your personal information adhere to the same privacy standards

We are committed to maintaining the highest standards of data privacy, security, and transparency. Should we use AI for processing personal information, which may have a legal impact on you, we will advise you accordingly.

Contact details and how to complain

We always welcome your queries regarding your personal information or privacy rights. You can reach us by writing to:

Data Protection Officer, Danske Bank, Donegall Square West, Belfast, BT1 6JS

Or email us at yourprivacyrights@danskebank.co.uk.

We strive to maintain a high standard of service. However, if you have concerns about how we manage your personal information or privacy rights, we are committed to addressing them promptly and effectively. If you wish to register a complaint, please provide detailed information, including your account details, a summary of your complaint, and any actions taken thus far. Use the contact details provided above.

Should you remain unhappy with how we managed your personal information, respected your privacy rights, or resolved your complaint, you have the right to complain to the Information Commissioner's Office. You can contact them by writing to:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF