

How we use your Personal and Business Information

Correct as at – 07 October 2026

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
- **People associated with an account**– Including beneficiaries, authorised signatories, guarantors, attorneys, parents, guardians, and others who give consent or are authorised to view or help manage an account

This notice applies to Northern Bank Limited trading as Danske Bank UK. We may share information with other companies in the Danske Bank Group as described in this notice.

The Bank has appointed a Data Protection Officer (DPO) who you can contact using the details at the end of this notice.



Your Rights

Under UK data protection law, you have certain rights regarding your personal information. Some rights apply only in certain circumstances:

- **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** – In certain circumstances, you can ask us to temporarily restrict how we use your personal information. This may affect our ability to provide an account or service
- **Right to Object to Processing** – You can object to us using your personal information where we rely on legitimate interests. We will stop unless we have compelling legitimate grounds that override your interests, rights, and freedoms, or we need the information to establish, exercise, or defend legal claims
- **Right to Data Portability** – In certain circumstances, you can ask us to provide personal information you gave us in a commonly used electronic format or transfer it to another organisation
- **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 object to direct marketing at any time. If you do, we will stop using your personal information for marketing purposes
- **Rights and Safeguards relating to Automated Decision-Making** – Where a decision is based solely on automated processing, including profiling, and produces a legal or similarly significant effect on you, you can request human involvement, make representations, and challenge the decision

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 using the details at the end of this notice.



Personal Information we collect

Depending on the services you use, or 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 your communications with us, including issued documents, notes, emails, phone calls, call transcripts and summaries, digital chats, and information generated through AI-assisted interactions. We may use automated and AI-assisted tools to analyse these records and may collect information about your interaction with our emails, such as whether you open an email or select a link

- **Technical Information** – Information about the device and technology you use to access our websites or banking applications, such as device identifiers, IP address, and operating system
- **Biometric Data** – Where relevant to a service or security purpose, we may temporarily retain photo IDs ('selfies') during some account-opening processes, design our applications to use biometrics available on third-party devices, and use behavioural biometrics, such as typing patterns and movement data, to enhance security and improve your experience
- **Video Recording** – Images captured when you visit our premises or 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, including where calls are recorded. We will tell you when recording takes 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 with your consent. Some marketing cookies are owned by third parties, such as Meta or Google. Depending on the cookie and how the information is used, we and the relevant third party may each have responsibilities under data protection law. 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
- Publicly available sources, including company registers and other publicly available business information, where relevant to our relationship with you or your business
- Other companies in the Danske Bank Group, where permitted by law and relevant to our relationship with you or your business
- 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 and the accuracy of information provided, and to 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, providing customer advice, administration, credit assessment, property valuation and managing credit risk and marketing. We do this to meet legal obligations, perform our contract with you, and pursue our legitimate interests, as applicable
- **Sharing information with third parties** – We share information where necessary to provide products or services, comply with legal or regulatory obligations, or pursue our legitimate interests, as applicable
- **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, support accurate processing, and maintain effective security arrangements, based on our legal obligations and legitimate interests
- **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 arrangements, legal obligations, and legitimate interests
- **To prevent fraud and financial crime** – We may use and share personal information to prevent, detect, investigate, and respond to fraud, scams, money laundering, terrorist financing, and other unlawful activity. We do this to comply with legal obligations and, where applicable, to pursue legitimate interests, including recognised legitimate interests provided for by data protection law

- **For profiling, market analysis, and relevant customer engagement** – We may analyse information we already hold and combine it with information from lawful public sources, including company registers, to understand market trends and customer needs, improve our products and services, and identify products or services that may be relevant. Where the activity is direct marketing, we will use the lawful basis required for that activity and respect your marketing preferences
- **To understand and improve customer interactions** – We analyse calls and other communications for quality assurance, employee coaching and training, complaint handling, operational insight, customer service improvement, reporting, compliance, and service efficiency. Depending on the purpose, we rely on contract, legal obligations, or legitimate interests
- **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 purposes including creditworthiness assessments, risk management, fraud prevention, promoting responsible lending and market protections. Depending on the specific purpose for which we process and share your personal information, we may rely on different lawful bases, including compliance with our legal obligations, our legitimate interests, or other lawful bases where applicable

Where we rely on legitimate interests, these may include improving customer service, safeguarding customers, preventing fraud, and financial crime, protecting

information and systems, monitoring service quality, training, and supporting employees, managing operational and business risks, administering our business, and developing or improving products and services. We balance these interests against the impact on you. You have the right to object to the processing as explained in the “Your Rights” section.

Criminal convictions and offences - We process information about criminal convictions and offences only where authorised by law and where necessary for purposes such as meeting legal or regulatory obligations, preventing or detecting unlawful activity, or establishing, exercising or defending legal claims.

We may collect and process sensitive personal information (also known as special category data), including information about health, racial or ethnic origin, sex life or sexual orientation, and biometric data used to identify you. We only collect and use this information where one of the following applies:

- With your explicit consent
- Where we are permitted to do so by the law, including where processing is necessary for reasons of substantial public interest.

Where we rely solely on your consent to collect and use sensitive personal information, you can withdraw that consent at any time. If you withdraw your consent, we might not be able to provide certain 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 help us manage your account, provide or protect your services, and meet contractual, legal, or regulatory obligations. Examples 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** – We may report or share information where required or permitted to prevent, detect, or investigate criminal or fraudulent activity
- **Payment service providers** – We share personal information to facilitate payments you wish to make, including identity verification
- **Payment schemes** – We share payment transaction information for reporting, industry analysis, service development, and benchmarking. Reports are aggregated and anonymised
- **Fraud prevention and industry fraud intelligence services** – We may share information with fraud prevention agencies, industry fraud intelligence services, payment service providers, other financial institutions, and relevant organisations where necessary to prevent, detect, investigate, or respond to fraud, scams, financial crime, or other unlawful activity
- **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 organisations that provide all or part of a service for us. They must protect your information and use it only as instructed or otherwise permitted by law
- **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, where we have your consent for direct marketing
- **Regulators** – We share information with regulators, such as the Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), and Information Commissioner's Office (ICO), to meet 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 use or share information for research and statistical purposes where permitted by law and subject to appropriate safeguards. Where possible, information will be anonymised



Transfer of personal data outside of the UK

Your personal information may be accessed or processed or stored outside the UK, including where third parties provide services on our behalf.

Where the country is covered by UK adequacy regulations, we may rely on the relevant adequacy regulations. Otherwise, we use appropriate safeguards, such as the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses or approved Binding Corporate Rules. For transfers to certified US organisations, we may rely on the UK Extension to the EU-US Data Privacy Framework.

We assess whether any additional safeguards are needed and require service providers to protect your information in accordance with applicable data protection law. You can read more about international transfers on the [ICO's website](#) or contact our Data Protection Officer for more information or to obtain a copy of our safeguards. Contact details are at the end of this notice.



How long we keep your personal information

We keep your personal information only for as long as needed for the purpose for which it was collected, or as required by law. Retention periods vary depending on the type of information, the product or service and the relevant legal or regulatory

requirements. We typically keep most information while you are a customer and may retain some information for up to seven years after your relationship with us ends for reasons including:

- **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 so that your identity cannot be recovered.



Profiling and automated decision-making

Profiling refers to a 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 assess credit risk, prevent money laundering and fraud, evaluate the likelihood of default, understand market trends and customer needs, and identify products or services that may be relevant to you. This may involve combining information we hold with information from public sources, such as company registers. Profiling may influence fraud checks, credit decisions or which products and services we consider relevant. Where profiling is used for direct marketing, we will use the lawful basis required for that activity and respect your marketing choices.

Automated decision-making is where we use your personal information, including profiling and credit reference information, to make a decision solely by automated

means, without human involvement. For example: this may affect whether an application is approved, declined, or referred for review, or whether a transaction is delayed or declined.

Where a decision is based solely on automated processing has a legal or similarly significant effect on you, you can request human involvement, make representations, and challenge the decision.



Use of Artificial Intelligence (AI)

We may use AI to help authorised colleagues review and summarise customer interactions, respond to customer queries, verify information using public sources, support quality assurance and employee training, and identify fraud or other risks. Where AI is used to support colleagues, its outputs do not replace appropriate human review.

Where AI processes personal information, we limit the information used to what is necessary and apply appropriate security, oversight and supplier controls. Where solely automated processing produces a legal or similarly significant effect on you, we will provide relevant information and the safeguards and rights described in the “Profiling and automated decision-making” section.



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. If you have concerns about how we manage your personal information or privacy rights, please contact us using the details above. To help us investigate, please provide relevant information about your concern and any action already taken.

If you remain unhappy with how we have handled your personal information, privacy rights, or 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