How we use your Personal and Business information – Potential Danske Bank UK Employees and Workers

Correct as at - 01 January 2025

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. However, you will always be provided with the most up to date version when making any application for employment.

This privacy notice applies to

- **Potential Employees –** All individuals applying for employment with Danske Bank UK, whether full-time, part-time,
  or temporary

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.

This notice does not form part of any contract of employment or other contract to provide services. It is important that all those applicable read this notice, so you are aware of how and why we process your personal information.

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. We will comply with your request unless there are compelling legitimate grounds for the processing which override your

interests, rights, and freedoms, or the processing is necessary for the establishment, exercise
or defence of legal claims

- **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

We will collect and process the minimum amount of personal information required about you to administer your application for employment with Danske Bank. This may include, but is not limited to, the following

- **Personal Contact Details** – Name and contact information (including addresses, phone numbers and email addresses)
- **Personal Information –** Date of birth and gender
- **Educational Background –** Including schools or universities attended, qualifications obtained, certifications or relevant training
- **Work Experience –** Previous employers, roles held, responsibilities in previous roles, employment durations and achievements
- **Skills –** Technical skills relevant to the role and soft skills (including communication, teamwork, problem-solving, etc.)

- **Recruitment Information –** Includes copies of interview record sheets, information on CV, references, application forms or cover letter explaining applicant's interest in the role
- **Proofs Supplied –** Proof of identity documents (such as, passport, driving licence, Immigration documents), proof of address, or right to work in the UK documentation
- **Other –** Details of any dependent or caring responsibilities
- **Legal and Regulatory –** Other information as necessary to comply with laws and regulations in respect of managing an employment application, which could include criminal conviction information

We may also collect and process the following 'special categories' of sensitive personal information, which may require your explicit consent to be held prior to collecting. These can include

- **Social Identities –** Information related to your race or ethnicity, nationality, religious beliefs, disabilities,
  and political opinions
- **Medical Information –** Includes information about your health status, medical conditions, medical certificates, and records related to health, and sickness
- **Personal Identifiers –** Biometric data (including voice recordings and psychometric assessments)

Providing accurate information is essential for administrating your employment application. 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 collect your personal information through various methods to ensure smooth administration of your employment application. These include

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

- During the employment application and recruitment process
- Notes and outcomes from interviews and pre-employment assessments

From third parties – This includes

- Information from criminal background checks, credit reports and reference checks
- From employment agencies
- Social media and public records

Why we collect and process your personal information

We pursue our legitimate interests to decide whether to appoint you to a role. We may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. We also need to process your personal information to decide whether to enter a contract with you.

We collect your personal information to

- Assess your skills, qualifications, and suitability for the role
- Carry out background and reference checks, where applicable
- Communicate with you about the recruitment process
- Keep records related to our recruitment process
- Comply with legal or regulatory requirements

We will process your personal information when

- Making a decision about your recruitment
- Determining the terms on which you work for us, if appropriate
- Checking you are legally entitled to work in the UK
- Administering any contract, we may propose to enter with you, if appropriate
- Ascertaining your fitness to work
- Complying with Health and Safety obligations
- To prevent fraud
- Equal Opportunities Monitoring
- Research purposes

We will only collect and 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 you consent, or where you have already made the information public

We will only collect and process sensitive personal information if any of the following is applicable

- With your explicit written consent
- Where we need to carry out our legal obligations, including compliance with employment laws
- If needed in the public interest, such as equal opportunities monitoring

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.

Third Parties that we Share Your Personal Information with

There are circumstances where we need to provide information to others to help us administer your employment application, 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 may share your personal information with other entities within the Group, to comply with group-based management requirements, including reporting on company performance, business reorganisation, group restructuring, or for system maintenance or data hosting
- **Third-party Service Providers –** Where required to provide IT services, security vetting administration, credit reference agencies and employment agencies. (Includes Cifas who use your personal information to prevent fraud, unlawful or dishonest conduct, malpractice, and other serious improper conduct. Further details can be found at www.cifas.org.uk/fpn or by contacting recruitment@danskebank.co.uk)
- **Financial Regulators or Certification Bodies –** Where required due to specific role requirements
- **Legal and Regulatory –** To comply with our reporting obligations under applicable laws and regulations

Sharing personal information with third parties is typically governed by data protection agreements to ensure compliance with data protection laws and to safeguard applicant's privacy and rights. Third-party sharing is always subject to appropriate security measures being in place to protect your personal information in accordance with our policies.

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 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 five years after we have communicated our decision regarding your application for a role, for the following reasons

- **Defence of any Legal Claim –** To respond to any legal claim, to establish that we have not discriminated against candidates based on prohibited grounds and that we have conducted the recruitment process in a fair and transparent manner
- **Research –** To analyse personal information for research purposes
- **Legal and Regulatory Compliance –** To comply with legislative and regulatory requirements, such as ensuring fair participation in employment as mandated by law

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.

Use of Artificial Intelligence (AI)

We are continuously striving to enhance our services and improve your experience when applying for employment. As part of this effort, we may implement artificial intelligence (AI) technologies in the future, although none are currently utilised.

If we decide to use AI technologies to process applicant's 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 and security. Should we decide to use AI for processing applicant's personal information we will advise you accordingly.

Contact Details and How to Complain

If you have any questions about this privacy notice or how the Bank processes your personal information you can write to the Bank at

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