

Danske Bank Privacy Notice – Potential Employees

Applicable for: Danske Bank A/S, London Branch

Effective from November 2025

Danske Bank Privacy Notice – Potential Employees

Authorised and regulated by the Danish Financial Services Authority (Finanstilsynet). Authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request. Registered Branch in England and Wales, Company No. FC011846, Branch No. BR000080. Danske Bank A/S. A public limited company incorporated in Denmark. CVR No. 61 12 62 28 Copenhagen



1. Introduction

This privacy notice applies to the processing of personal data of candidates for employment with Danske Bank A/S, London Branch (candidates are referred to in this privacy notice as potential employees).

Danske Bank is the data controller for the processing of the personal data covered by this privacy notice.

We want to inform you, as a potential future employee of Danske Bank, about "when, what and why" we process your personal data, as well as your rights concerning that data. We take all relevant measures to protect your data and privacy in accordance with applicable legislation during the recruitment process.

This privacy notice details the basis on which Danske Bank processes your personal data, along with the privacy rights you are entitled to by law.



2. What personal data do we process?

We process various types of personal data, including the following:


- CV, psychometric and cognitive tests results, interview records, and other application documents, including previous professional experience and qualification, educational level, year of graduation, and positions of your interest in Danske Bank.
- Professional memberships, diplomas, transcripts, languages, computer skills, national service completion (if applicable), identification number.
- Name, gender, date of birth.
- Citizenship, home/term private address, personal email address and other contact details.
- Where applicable, information about your former employment within the Danske Bank Group, such as reasons and grounds for termination, termination date, warnings, assessments of your performances and other information related to your status as a former employee.
- Any additional personal data you provide to us during interviews.



3. Our purposes and legal basis for processing your personal data

We process your personal data for various reasons related to recruitment, employment, and fulfilling our legal obligations. These include:

- **Recruitment and Candidate Assessment:** We process your personal data, such as CV, test results, interview records, psychometric testing results and other application documents, to assess you as a candidate and potentially include you in our recruitment database. This processing is necessary to take steps at your request prior to entering into a contract [see UK GDPR article 6.1(b)] and to pursue our legitimate interests in ensuring fair and successful recruitment processes [see UK GDPR article 6.1(f)].
- **Legal Obligations:** We fulfil legal obligations, such as complying with anti-money laundering and right to work in the UK legislation, which requires processing certain personal data like name, gender, date of birth, citizenship, and contact details. This processing is based on compliance with legal obligations [see UK GDPR article 6.1(c)].
- **Former Employment within the Group:** For former employees, we process information about your previous employment within the Group, including reasons and grounds for termination, termination date, warnings, and assessments of your performance. This is necessary for maintaining accurate records and fulfilling legal or contractual obligations [see UK GDPR, articles 6.1(c) and 6.1(b)].



In some cases, the Danske Bank Group requests your consent for processing your personal data. Before you give your consent, you will receive information about the specific processing activity to ensure clarity about what you are consenting to. For example, the Group processes your email for job notifications based on your consent (see UK GDPR, article 6.1(a)). You may withdraw your consent at any time.



4. Third parties and your personal data

Personal data collected from third parties

We collect personal data from third parties for various purposes. These third parties can include:

- Recruitment, executive and non-executive search companies. The personal data we receive includes your name, contact details, CV, feedback from test/assessments conducted by third parties and other application documents.
- Publicly accessible sources, such as LinkedIn, when you provide a link during the recruitment process. The personal data we collect includes your full name, email, work history, and other information included in your profile.
- Former employers, subject to the references you provide. The personal data we receive includes assessments of your performances.
- Background screening companies and credit reference agencies. This processing is based on compliance with legal obligations, for example under the senior managers and certification regimes (see UK GDPR article 6.1(c)) and to pursue a legitimate interest (see UK GDPR article 6.1(f)).

Personal data shared with third parties

In some instances, we share personal data with third parties outside the Danske Bank Group, and such third parties may share personal data with each other:

- Recruitment, executive and non-executive search companies receive personal data about you, such as employment conditions, to complete the recruitment process.
- When performing background checks on final candidates. Note that for certain positions this may include criminal record checks, for example, for applicants for regulated positions under the Senior Managers regime.
- Third-party service providers appointed as data processors to perform functions and services on our behalf, who are not authorised to use such data for any other purposes (e.g., providers of software for recruitment databases, administration services, etc.)



5. Processing of personal data and AI-systems

While we may employ AI tools to assist with the recruitment process and this may include the use of your personal data, you will not be subject to decisions based solely on automated decision-making or AI.

The legal basis for this processing is to pursue a legitimate interest (see UK GDPR article 6.1(f))



6. Special categories of personal data

We will only use special categories of your personal data where we are permitted by law to do so.



Types of special category personal data

We may process the following types of special category personal data

- Information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- Information about your nationality or ethnicity, to assess whether a work permit and a visa will be necessary for the role.

We also process special category personal data that may appear or be inferred from the information you give us.

Legal basis for processing special category personal data

We may process special category personal data about you on the legal basis of

- Your explicit consent (see UK GDPR article 9.2(a))
- To establish or to fulfil a contract with you (see UK GDPR article 6.1(b)), or
- The establishment, exercise or defence of legal claims (see UK GDPR article 9.2(f))



7. Transfer of your personal data outside the UK

Some third parties that we share personal data with may be located outside the UK and the Danske Bank Group's main data hosting sites are within the European Economic Area.

When Danske Bank transfers your personal data to third parties outside the UK, we ensure that your personal data and data protection rights are subject to appropriate safeguarding by

- Ensuring that there is an adequacy decision by the United Kingdom government, or
- Using standard contracts approved by the Information Commissioner's Office.

You can get a copy of the standard contract by contacting us (see contact details in section 11).



8. For how long do we store your personal data?

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. The personal data will subsequently be deleted or irreversibly anonymised.

If you are successful in your application and become an employee of Danske Bank, we will retain your personal data in accordance with the Danske Bank Privacy notice for employees. If you are unsuccessful we will retain your personal data for 6 months or for a period of 3 years upon your explicit consent. We retain your personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way.

We further retain such personal data with your consent in case a similar role becomes vacant for which you will be a fitting candidate.

Surveillance videos for our entrance and reception areas are deleted 30 days after they were made. In certain circumstances, and in connection with a specific case, the information may be stored for a longer period.



9. Your rights

Your rights in relation to personal data are described below. To exercise your rights, you can

- Contact us on our main telephone number [+44 20 7410 8000]
- Get in touch with your point of contact in the Human Resources Department either directly or by calling the number above

See section 11 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. You can obtain information about the period for which we store your data and about who receives data about you, to the extent that we disclose data in the UK and abroad. Your right of access may, however, be restricted by legislation, protection of other persons' privacy and consideration for our business and practices. Access to video surveillance may be restricted due to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding of 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.

You can make an access request by contacting us as specified above.

Right to object

In certain circumstances, you have the right to object to the processing of your personal data. This is the case, for example, when the processing is based on our legitimate interests.

Right to rectification of your data

If your personal data is inaccurate, you are entitled to have the personal data rectified. If 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 in relation to the purposes for which it was collected.

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

- For compliance with a legal obligation, for instance if we are obliged by law to hold your personal data for a certain period of time. In such situations, we cannot erase your data until that time has passed.
- For the performance of a task carried out in the public interest.
- For establishment, exercise or defence of legal claims.

Restriction of use

If you believe that the personal data we have registered about you is incorrect or if you have objected to the use of the personal data, you may demand that we restrict the use of the personal data to storage until the correctness of the personal data can be verified or it can be checked whether our legitimate interests outweigh your interests.

If you are entitled to have the personal data we have about you erased, you may instead request us to restrict the use of the personal data to storage. If we need to use the data solely to assert a legal claim, you may also demand that any other use of the personal data be restricted to storage.



Withdrawal of consent

Where consent is the legal basis for a specific processing activity, you may withdraw your consent at any time. Note that we will continue to use your personal data, for example to fulfil an agreement we have made with you or if we are required by law to do so.



10. Changes to this privacy notice

We are required to update this privacy notice on a regular basis. In case of a change, the 'effective from' date at the top of this document will be amended. If changes to how your personal data is processed will have a significant effect on you personally, we will take reasonable steps to notify you of the changes to allow you to exercise your rights (for example to object to the processing).



11. 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 your personal data.

You can contact us on our main telephone number [+44 20 7410 8000]. You are also welcome to contact the Human Resources Department.

You can contact our Data Protection Officer by email at dpofunction@danskebank.com or by post at: Data Protection Officer, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark.

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 contact our complaints handling unit – Danske Bank, Legal Department, 75 King William Street, London EC4N 7DT. You can also lodge a complaint with the UK Information Commissioner's Office (further details are available on www.ico.org.uk or by calling 0303 123 1113).