Danske Bank Privacy Notice – Potential Employees – Irish Branch

Effective from 8 December 2025

Introduction

This privacy notice outlines the processing of personal data by Danske Bank A/S ("Danske Bank" and its company group the "Group") as data controllers. We want to inform you, as a potential future employee of the Group 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.

This privacy notice details the basis on which legal entities and branches within the Group process your personal data along with the privacy rights to which you are entitled by law.

What personal data do we process?

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

- CVs, personality and cognitive test results, interview records and other application documents, including previous professional experience and qualifications, education level and year of graduation, and the positions of interest to you within the Danske Bank Group;
- Name, gender, date of birth;
- Citizenship, private address and other contact details;
- information about your former employment within the Group (if applicable), such as reasons for and grounds for termination, termination date, warnings, assessments of your performance and personality and other information related to your status as a former employee.

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 your CV< test results, interview records 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 (cf. GDPR art. 6.1(b)) and to pursue our legitimate interest in ensuring a fair and successful recruitment process (cf. GDPR art. 6.1 (f) }
- Legal Obligations: We fulfil legal obligations such as complying with anti-money laundering legislation which requires processing certain personal data such as name, date of birth, citizenship and contact details. This processing is based on compliance with legal obligations cf. GDPR art 6.1© and relevant national legislation concerning financial regulation.
- Former Employment within the Group: for former employees, we process information about your previous employment within the Group, including reasons for and grounds for termination, termination date, warnings, and assessments of your performance and personality. This is necessary in order to maintain accurate records and to fulfil legal or contractual obligations (cf GDPR art. 6.1 © 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 (cf. GDPR art 6.1(a)). You may withdraw your consent at any time and you will be informed about the consequences of such withdrawal.

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, etc., when you provide a link during the recruitment process. The personal data we collect includes your full name, email address, 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 and personality.

Personal data shared with third parties

In some instances, we share personal data with third parties inside or outside the Group, and such third parties may share personal data with each other. They include:

- 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 for critical positions covered by regulations such as anti-money-laundering and anti-terrorism-financing checks
- 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 outside these functions and services (e.g. as providers of software for recruitment databases, administration services etc.)

Transfer of your personal data to third countries

We are committed to ensuring the security of your personal data. For this reason, we prioritise that our main data hosting lies with the EEA, leveraging on data centres with robust security measures. To the extent that we transfer your personal data to a business partner outside the EEA< we are committed to ensure that our transfer or your personal data is conducted in accordance with GDPR Chapter V. We have suppliers in countries that appear on the European Commission's list of safe countries (countries that have received an adequacy decision).
As part of our operations, we may in a few cases transfer your personal data to recipients who are located in an unsafe third country (not subject to an adequacy decision from the European Commission). In these cases, we generally apply Standard Contractual Clauses with appropriate supplementary measures implemented when necessary to ensure that the transfers are subject to appropriate safeguards under the GDPR.
Where relevant to the context of our engagements with you and processing of your personal data, your information is transferred to our IT partner Infosys in India for the provision of agreed services to Danske Bank. We have documented that we have no reason to believe that the relevant legislation will be interpreted or applied in practice in a way that would affect the transferred personal data or compromise the protection required under the GDPR.

Your personal data may also be transferred to an unsafe third country in support cases where an emergency makes it necessary for us to utilise support outside the EEA to obtain what is known as "follow the sun support" from our vendors' specialised employees located in various countries. Such transfers i.e. remote view/screen sharing access, only occurs when absolutely necessary. Support requests and remote access typically do not include your personal data. However, if unresolved issues require vendor support involvement, Danske Bank employees may, in exceptional circumstances, determine that sharing a screen shot containing your personal data or engaging in video calls where vendors can view your personal data is necessary during the support process, although your personal data is not the main focus in the support

procedure. If you wish to know which IT vendors may process information about you in third countries, you can contact hr-services-support@danskebank.dk to obtain a list.

Your rights

Your rights regarding personal data are detailed below. To exercise these rights you may contact us through the following channel: hr-services-support@danskebank.dk.

Please refer to the section "Contact Details and how to submit a complaint" for further information on contacting Danske Bank about data protection.

Insight into your personal data

You have the right to obtain insight into the personal data we process, where it comes from and the purpose of the processing.

This includes obtaining information regarding how long we store your personal data and who receives your personal data, to the extent that we disclose personal data in Ireland and abroad. Your right to insight may, however, be restricted by legislation, obligations to protect the privacy of others and consideration for our business and practices. Our know-how, business secrets as well as internal assessments and material may also be exempt from the right of insight.

Correction or erasure of Danske Bank Group's data

If the personal data we hold about you is incorrect, incomplete or irrelevant, you are entitled to have it corrected or erased, subject to any legal restrictions and rights to process data. These rights are known as the "right to rectification", "right to erasure" or "right to be forgotten".

We retain your personal data only for as long as necessary for the purpose for which it is processed or if there is a specific regulatory or contractual reason to keep it for longer than its fulfilment of the original purpose. We typically save your personal data for up to six years during and following your employment and in specific cases, even longer. This is because the personal data may be used by the Group to exercise or defend against a legal claim. Different types of personal data may be erased at different times depending on when they are no longer needed.

Restriction of use and the right to object

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

If the Group is processing your personal data based on legitimate interest, you have a right to object to that processing.

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

Withdrawal of consent

If we process personal data based on your consent, you can withdraw your consent.

Data portability

You have a right to receive the copy of the personal data you have provided in an electronic machine-readable format if the legal basis of processing is consent or performance of a contract.

Erasure and retention of personal data

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 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).

Contact details and how to submit a complaint

You are always welcome to contact us, regarding your privacy rights and how we process your personal data. Contact our Data Protection Officer as follows:

DPO, Danske bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark. e-mail: dpofunction@danskebank.com.

Please also copy the Ireland Branch Data Protection Information Contact whose contact details are as follows:

Data Protection Information Contact, 7th Floor, The Shipping Office, 20-26 Sir John Rogerson's Quay, Dublin 2, D02 Y049.

You can also contact our Data Protection Officer with 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 register and use your personal data and if your dialogue with the DPO has not led to a satisfactory outcome for you, contact our complaints handling unit: Danske Bank, Group HR Legal, Berstorffsgade-40 DK-1577 Kobenhavn V, Denmark.

You can also lodge a complaint with the Irish Data Protection Commission: Canal House, Station Road, Portarlington, R32 AP23 Co. Laois, email: info@dataprotection.ie phone: +353 (0) 57 8884800 or +353 (0) 761 104 800.