Danske Bank Privacy Notice – Potential Employees

Applicable for: Danske Bank A/S Finland, Danske Invest Fund Management Ltd, Danske Mortgage Bank Plc

Effective from 1st of January of 2026

1. Introduction

This privacy notice outlines the processing of personal data by Danske Bank A/S, Finland Branch (1078693-2), Danske Invest Fund Management Ltd (0671602-6) and Danske Mortgage Bank Plc (2825892-7) (later “Danske Bank” or the “Group”).

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 during the recruitment process.

This privacy notice details the basis on which legal entities and branches within the Group process 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 about you, including.:

- CV, personality 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 the Danske Bank Group.
- Name, gender, date of birth.
- Citizenship, private address and other contact details.
- Credit information

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, 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 interests in ensuring fair and successful recruitment processes, cf. GDPR, art. 6.1(f).
- Legal Obligations: We fulfil legal obligations, such as requirements for work permits and, where applicable, residence permits, as well as compliance with anti-money laundering 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, cf. GDPR, art. 6.1(c), and relevant national legislation concerning financial regulations.
- Security clearance (Suojelupoliisi background check): We process your personal data to conduct mandatory security clearance checks (turvallisuusselvitys) for positions that involve the prevention of money laundering, terrorist financing or other roles requiring a high level of reliability and integrity. This processing is required under the Finnish Security Clearances Act (726/2014) and financial sector regulations obligating banks to ensure the

suitability and trustworthiness of individuals in certain critical positions. The processing is based on compliance with legal obligations, cf. GDPR art. 6.1(c), and applicable national legislation.

- Credit check: We process your personal data to carry out credit checks when required accordance with the Finnish Act on the Protection of Privacy in Working Life (759/2004), which permits employers to obtain such information. The processing is based on our legitimate interest in ensuring the reliability and suitability of candidates for such positions, cf. GDPR art. 6.1(f), and applicable national legislation.
- Drug testing: We process your personal data for the purpose of conducting a drug test. A drug test is carried out only for the candidate selected for the position. The employer is entitled to require a drug test in accordance with the Finnish Act on the Protection of Privacy in Working Life (759/2004). The processing is based on compliance with legal obligations, cf. GDPR art. 6.1(c), and applicable national legislation.

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 of any consequences of such withdrawal.

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 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 outside the 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 for critical positions covered by regulations such as anti-money laundering and anti-terrorism financing.
- Credit information companies: The credit assessment company receives your name and date of birth, and, if necessary, your personal identification number, in order to identify you and provide a credit assessment to Danske Bank.
- 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. Transfer of your personal data to third countries

We are committed to ensuring the security of your personal data. For this reason, we prioritize that our main data hosting lies within the EEA, leveraging on data centres with robust security measures. To the extent we transfer your personal data to a business partner outside the EEA, we are committed to ensure that our transfer of 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 third countries (countries that have received an adequacy decision).

As part of our operations, we may in a few cases transfer your 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 utilize 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 henkilöstöpalvelut@danskebank.fi to obtain a list.

6. Your rights

Your rights regarding personal data are detailed below. To exercise these rights, you may contact us through the following channel:

- Contact us via email: henkilöstöpalvelut@danskebank.fi

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 your personal data in Finland 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 data

If the data we hold about you is incorrect, incomplete, or irrelevant, you are entitled to have the data 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 keep your data only for as long as it is needed for the purpose for which your data were processed. Thus, we will save your personal data during the recruitment process and up to six months from the ending date of the recruitment process. Our reason for saving your personal data is because it may be used by the Group to defend against a legal claim.

Restriction of use

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 these data to storage. Use will only be restricted to storage until the correctness of the personal 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 these 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 at any given time.

Data portability

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

7. Changes to this privacy notes

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 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).

8. 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 at dpofunction@danskebank.com.
- If dissatisfied with how we register and use your personal data, and your dialogue with the Data Protection Officer has not led to a satisfactory outcome, contact our complaints handling unit: Danske Bank, HR Legal FI, Televisiokatu 1, 00240 Helsinki / hrlegalfinland@danskebank.fi

- You can also lodge a complaint with the Office of the Data Protection Ombudsman, P.O. Box 800, 00521 Helsinki; email: tietosuoja@om.fi.