



Danske Bank Privacy Notice – Potential Employees

Applicable to: Danske Bank A/S, Danmark, Sverige filial

Effective from May 2026



1. Introduction

As potential future employee of Danske Bank A/S, Danmark, Sverige filial we want to inform you of the bank's processing of your personal data and your rights. We process your data since it is in our legitimate interest to complete a fair and successful recruitment process. Further, personal data is necessary for us to potentially enter into an employment agreement with you. We may also process your personal data if you explicitly consent to the process.

We protect your data and privacy by taking all relevant measures in accordance with applicable legislation.

This privacy notice sets out the basis for how legal entities and branches within Danske Bank Group (the "bank") look after your personal data and the privacy rights you are granted by law.



2. What personal data do we process?

We process different kinds of personal data about you, e.g.:

- CV, application letter, tests, diplomas, interview records and other application documents, including credit reference and bank account number, previous work history, assessments and evaluations, educational level and year of graduation.
- Name, gender, personal ID number and salary request.
- Nationality, private address and other contact details.
- Publicly available information, including information on social networks.



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

We process your personal data for the following purposes:

- Recruitment and non-executive searches. We have a legitimate interest to process application documents such as CV, application letter, assessment and evaluation, credit reference work history and educational information and personality tests in order for the recruitment process to be fair and successful and to comply with legal requirements. We also have a legitimate interest to check publicly available information on you in the screening process, for example if it is necessary for the position to review information about you on social networks to be able to assess specific risks for a specific position. Further, our processing of such data is necessary in order to eventually enter into an employment agreement with you and/or to inform you about vacancies in the future.
- If you have applied for a managerial position within the bank, we are legally obliged to conduct consultations with the trade unions that are parties to our collective bargaining agreements prior to your employment.



4. Third parties and your personal data

Personal data collected from third parties

We process personal data from third parties, for instance from:

- Recruitment and executive search companies and the Credit Agency. The personal data we are provided are e.g. your name, contact details, CV, credit reference and other applicant documents. The personal data may be collected

from your publicly available information on job profiles on social medias e.g. LinkedIn. The bank has a legitimate interest to ensure the recruiting process is fair and successful.

- Former employers subject to the references provided by you. The personal data we are provided are e.g. assessments of your performances and personality.

Personal data shared with third parties

In some instances, we may share personal data with third parties inside or outside Danske Bank Group:

- Recruitment and executive search companies receives personal data about you such as employment conditions in order to complete the recruitment process.
- If you have applied for a managerial position within the bank, the trade unions that are parties to the collective bargaining agreement with the bank will receive personal data about you in order to carry out our legal obligation to consult the trade unions prior to your employment.



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 hr-services-support@danskebank.dk to obtain a list.



6. Your rights

Insight into your personal data

You can obtain insight into the personal data we process, where it comes from and what we use it for. You can obtain information about for how long we store your data and about who receives data about you, to the extent that we disclose data in Sweden and abroad. Your right of access may, however, be restricted by legislation, protection of other persons' privacy and consideration for our business and practices. Our know-how, business secrets as well as internal assessments and material may also as such be exempt from the right of insight.

Correction or erasure of data

If the data is incorrect, incomplete or irrelevant, you are entitled to have the data corrected or erased with the restrictions that follow from existing legislation and rights to process data. These rights are known as the "right to rectification", "right to erasure" or "right to be forgotten".

Restriction of use

If you believe that the 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 data can be established, or it can be checked whether our legitimate interests outweigh your interests.

If you are entitled to have the 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 to disclose data at any given time. However, this may prevent us from continuing the recruitment process with you.

Please note also that we will continue to use your personal data if we have another legal ground for the processing, e.g. a legitimate interest as mentioned in the General Data Protection Regulation (GDPR).

Data portability

If we use data based on your consent or as a result of an agreement, and the data processing is automated, you have a right to receive the copy of the data you have provided in an electronic machine-readable format.



7. Erasure and retention of personal data

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 two years from the ending date of the recruitment process. The reason we save your personal data is so that the bank can use it to defend itself against a legal claim.



8. Contact details and how to submit a complaint



You are always welcome to contact us, as data controller, if you have questions about your privacy rights and how we register and use personal data. You can contact our Data Protection Officer by email at dpofunction@danskebank.com. If you are 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, you can contact our complaints handling unit: Danske Bank, HR Legal Department, Norrmalmstorg 1, 103 92 Stockholm. You can also lodge a complaint with the Swedish Authority for Privacy Protection (Sw.*Integritetsskyddsmyndigheten (IMY)*): Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm, e-mail: imy@imy.se.