

Danske Bank Privacy Notice – Potential Employees

Effective from 1 January 2026



Introduction

This privacy notice outlines the processing of personal data by Danske Bank A/S S.A. Branch in Poland (KRS 0000250684) address at Wspólna 70, 00-687 and Danske bank A/S (CVR 61126228) address Bernstorffsgade 40, DK-1577 København V, Denmark ("Danske Bank" or 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 during the recruitment process.



What personal data do we process?

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

- CV, results of tests, interview records and other application documents, including previous professional experience and qualification, employment track record, results of tests, interview records and other application documents educational level and year of graduation, and positions of your interest in the Danske Bank Group;
- name (names) and surname, date of birth, contact details given by the candidate,
- citizenship, contact details given by the candidate.
- information about your former employment in the Group, such as reasons and grounds of termination of your employment, termination date, warnings, assessments of your performances and personality, other information about you 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 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 complying 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.
- **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 and personality. This is necessary for maintaining accurate records and fulfilling legal or contractual obligations, cf. GDPR, art. 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, 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.



Third parties and your personal data

Personal data collected from third parties

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

- recruitment, executive and non-executive search companies. The personal data we are provided are e.g. your name, contact details, CV, feedback from test/ assessments conducted by third parties and other application documents.
- from publicly accessible sources, such as Pracuj.pl, LinkedIn, etc., in case you provide us a link during recruitment process. The personal data we are collecting is full name, email, work history, and other data included on you profile;
- 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 the Group and such third parties may share personal data with each other:

- recruitment, executive and non-executive search companies may receive personal data about you, such as employment conditions, in order to complete the recruitment process.
- when we perform background checks on our finale candidates for critical positions covered by e.g. anti-money-laundering and anti-terrorism-financing
- third party service providers who have been appointed as data processors to perform functions and services on our behalf and are not authorised by us to use such data for any other purposes (e.g. providers of software for recruitment database, administration services and etc.)



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.



Your rights

Your rights regarding personal data are detailed below. To exercise these rights, you may contact us through the following channel: [Please adjust as per your market area]

- Contact us via email: 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 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 Poland, Denmark, Lithuania 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 as such may also as such be exempt from the right of insight.

Correction or erasure of Danske Bank Group's 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 and the right to object

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 in your personal data not being processed.

If the Group is processing your personal data based on legitimate interest, you have a right to object to that processing. Please contact the Talent Acquisition team or HR Legal if you wish to exercise this right to object.

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. Please note that we will continue to use your personal data if we have another legal ground for the processing, e.g. a legal or contractual obligation.

Data portability

You have a right to receive a copy of the data you have provided in a structured, commonly used and machine-readable format if the processing of those data is based on your consent or in order to entering into a contract.



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 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.



Contact details and how to submit a complaint

You are always welcome to contact us, regarding your privacy rights and how we process personal data. You can contact our Data Protection Officer, e-mail:

- Contact our Data Protection Officer 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, Group HR Legal, Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark.
- You can also lodge a complaint with the Danish Data Protection Agency: Datatilsynet, Borgergade 28, 1300 Copenhagen K, e-mail: dt@datatilsynet.dk or with the Polish Data Protection Authority: - the President of the Personal Data Protection Office in Poland (Prezes Urzędu Ochrony Danych Osobowych) at: Stawki 2 str., 00-193 Warszawa - if you believe that the processing of your personal data violates the law.