

Realkredit Danmark A/S's privacy notice for personal customers and private individuals

Effective from 18 September 2026

1. Introduction

This privacy policy describes how Realkredit Danmark processes your personal data.

Realkredit Danmark is the data controller for the processing of the personal data set out in this privacy notice.

Realkredit Danmark A/S, CVR no. 13399174, Bernstorffsgade 40, 1577 Copenhagen V.

Data Protection Officer (DPO) contact details:

Data Protection Officer, Realkredit Danmark A/S, Bernstorffsgade 40, 1577 Copenhagen V, email: dpofunction@rd.dk.

This privacy policy applies to personal customers, potential personal customers, sole proprietorships, other third-party individuals such as guarantors, holders of powers of attorney and persons connected to or associated with a business customer; it also applies to institutions and the individuals representing them, including authorised signatories, beneficial owners, directors, employees, holders of powers of attorney, guarantors, pledgers and other third parties connected to a business customer, as well as representatives of business customers with whom we are in dialogue or cooperate.

Please note that we have separate privacy policies that apply to members of the board of directors, executive management, employees in key functions and persons closely related to them.

2. Which personal data do we process?

Depending on the products and services you have ordered or are interested in, we process different kinds of personal data, including

- identification information, such as your name, social security number or other national ID number, country of residence, residence and work permit information, PEP status (political exposure status) and proof of identity, such as a copy of your passport, driver's license, national health insurance card or birth certificate.
- contact information, including your address, telephone number and email address.
- financial information, including information about your income, assets, debts, credit assessment, insurances, pensions, taxes, environmental impact, bankruptcy information and members of your household (number and age of persons).
- estate and inheritance management information.
- property and other collateral, including market value, energy data and environmental aspects.
- information about your education, profession, employment and experience.
- information about your family and household.
- information about the products and services we provide to you or our business customer.
- other personal data as necessary to provide you or you or our business customer with specific products or services, or if we are required by law to do so.
- personal data relating to information about upcoming or past business/personal anniversaries or life events

e.g. retirement days, birthdays, special preferences etc.

- information on how you use our products and services and your preferences in relation to these.
- digital information related to your use of our websites, platforms and digital applications, including traffic data, location data, behavioural data and other communication data; for example, information collected by use of cookies on our websites.
- tracking data from newsletters if you have consented to this when signing up for newsletters.
- information about your devices used to access our websites, platforms and digital applications as well as technical information, including information on the type of device and operating system.
- information provided by you about your preferences for various types of marketing and events.
- recordings of conversations and online meetings, cf. [Recording of conversations and of online meetings](#).
- transcriptions and summaries of discussions with you during online meetings and in-person meetings using AI Technology, cf. [Automatic transcription and meeting minutes](#).
- Information relating to a customer being deceased, including data processed in connection with the administration and closure of products and/or services to a deceased customer.
- video surveillance of the front of buildings and entrances to our premises and Danske Bank branches in which the advisers are based, as well as reception and customer areas.

- if you are a sole trader – company name and identifier, company number, VAT Number. Information relating to ownership and ownership structure for a privately owned company, information of other relations to the company, e.g. board member(s), manager as well as, general information about your business.
- For sole traders and business customers, data on the environmental, social and governance (ESG) impact of your business in the environment in which it operates.
- legal and investigative information – e.g. court decision, fines, witness statements, financial crime investigation.
- relationship and corporate information – e.g. relation to company, relation to other banks and membership in boards.

Our ability to offer the best advice and solutions for you very much depends on how well we know you. Consequently, it is important that the information you provide is correct and accurate and that you inform us of any changes. See section 13 for more information on how to contact us so that we can help you make any necessary corrections.

3. What do we use your personal data for?

We process personal data about you to offer you the best advice and solutions, to protect you against fraud, to fulfil our agreements with you and to comply with applicable regulations, including data security.

We process your personal data to provide you with the financial services or products you have requested, including

- mortgage loans
- fixed-price agreements
- registration services
- guidance and advice on loans
- payment services
- digital solutions
- insurance products
- loan monitoring

We process personal data for the following purposes:

- To enable us to offer you, as a potential customer, our products and services, and, if you choose to accept one or more of our products or services and become a customer, for onboarding purposes in relation to identification and verification for anti-money laundering purposes. For people connected or associated with a business customer, we process the information to verify your identity when we register you in our systems and as part of our anti-money laundering activities.
- Customer services and customer relationship management, including advice, administration, credit assessment, recovery of outstanding debt, handling of complaints and making information available to service providers authorised to request information about you.
- Communicating with you about your or the business customer's products and services for legal, regulatory and service purposes.
- Improving, developing and managing our products and services and setting fees and prices for our products and services, including using data analytics and statistics to improve products and services and testing our systems, as well as developing, training and testing models.
- Countering potential and actual fraud, including the processing of behavioural data, for the purpose of detecting and preventing suspicious activity in connection with your mortgage loan.
- Enabling Realkredit Danmark, Danske Bank or third parties to pursue statistical, scientific and research purposes as part of research projects or similar, including anonymisation of personal data for such purposes.
- Loan monitoring of your mortgage loan as well as interest rate and price trends so that we can inform you of your options, if you use this service.
- Marketing of our products and services, including marketing on behalf of other entities of the Danske Bank Group, provided we have obtained your consent or are allowed to perform such marketing activities by law.

- Distribution of newsletters, such as articles, news and updates, if we have obtained your consent. We may also invite you to events and send you other marketing material based on your preferences if we have your consent to this.
- We use cookies on our websites and in our digital apps for functional, statistical and marketing purposes via digital channels and social media platforms, such as Facebook, if you have consented to this. Please refer to our [cookie policy](#) for more information.
- To comply with applicable law, including statutory disclosures, and for other regulatory and administrative purposes, including identification and verification as stipulated in the Danish Anti-Money Laundering Act, risk management, and prevention and detection of money laundering, fraud and other types of financial crime. In relation to anti-money laundering measures, identification data is collected at regular intervals during your customer relationship with us as required by law, or as long as the business customer you are connected or associated with is a customer with us.
- Checking, testing and monitoring our compliance with internal policies and rules, regulatory and legislative requirements, for example in relation to data protection, financial crime or market integrity.
- To develop, maintain and use models for credit risk exposure and Internal Ratings-Based (IRB) modelling for the assessment of capital requirements under the Capital Requirements Regulation (CRR), which is a required element of Realkredit Danmark's risk management, and to share information between entities within the Danske Bank Group for these purposes with appropriate justification under the Danish Financial Business Act.
- Security and crime prevention, including the use of video surveillance of the front of buildings, entrances to the branches of the Danske Bank Group and other premises, reception and customer areas, ATMs and counters.
- Determining the total loan volume broken down by energy performance rating and calculated carbon emis-

sions. We also use the calculation for statistical purposes, including calculation of the carbon footprint of financed activities at Realkredit Danmark.

- Documenting our total issuance of green mortgage bonds, for example Cbor6®Green bonds, in accordance with the terms applicable to such bonds.

4. What is our legal basis for processing your personal data?

We must have a legal basis to process your personal data.

The legal basis will be one of the following:

1. You have given us consent to processing your personal data for a specific purpose, cf. the General Data Protection Regulation (GDPR) art. 6.1(a).
2. You have entered or are considering entering into an agreement with us on a service or product, cf. GDPR art. 6.1(b).
3. Due compliance with a legal obligation, cf. GDPR art. 6.1(c), for example, in accordance with
 - the Danish Anti-Money Laundering Act (*hvidvaskloven*)
 - the Danish Tax Reporting Act (*skatteindberetningsloven*)
 - the Danish Bookkeeping Act (*bogføringsloven*)
 - the Danish Credit Agreements Act (*lov om kreditaftaler*)
 - the Danish Financial Business Act (*lov om finansiel virksomhed*)
 - the Danish Payments Act (*betalingsloven*)
 - the Danish Marketing Practices Act (*markedsføringsloven*)
 - the GDPR and the Danish Data Protection Act (*dataskyttelsesloven*)
 - the Danish Capital Markets Act (*lov om kapitalmarkeder*)
 - the EU Capital Requirements Regulation (CRR)
 - the EU Markets in Financial Instruments Regulation (MiFiD I & MiFiD II)
 - the EU Market Abuse Regulation (MAR)
 - the Danish Administration of Justice Act (*retsplejeloven*)

- the Danish Civil Registration System Act (*CPR-loven*)
- the Danish TV Surveillance Act (*TV-overvågningsloven*)
- the Danish Mortgage-Credit Loans and Mortgage-Credit Bonds Act (*lov om realkreditlån og realkreditobligationer*) and associated orders
- the Danish Land Registration Act (*tinglysningsloven*)
- The Danish Act on Protection of Whistleblowers

4. It is a prerequisite for pursuing Realkredit Danmark's and/or Danske Bank's legitimate interests, cf. GDPR art. 6.1(f). For example, this may be for (i) documentation and security purposes, (ii) to prevent and detect money laundering, fraud, abuse and loss, (iii) to strengthen IT and payment security and to develop and test new IT systems and/or (iv) for direct marketing purposes.

We will do so only if our legitimate interest in each case is not outweighed by your interests or rights and freedoms.

5. Special categories of personal data

Some of the data we have on you may be explicitly delimited in the GDPR, and as the right to process such data is more restricted than for general data, it will be processed only when necessary. In some instances, however, it is necessary to process special categories of personal data about you. Typically, such processing will take place when the data can be deduced from a review of budget information, applications and other forms related to your order of our products and services.

Below, you will find examples of types of special categories of personal data we process about you, the purpose of the processing and our legal basis (exceptions set out in GDPR art. 9) for doing so.

Types of special categories of personal data

- Trade union membership in connection with certain loan products, discount plans and review and documentation of your budget in connection with an application.

- Data on your religious or philosophical beliefs or political opinions in connection with the review and documentation of your budget in connection with an application.

Purpose and legal basis

We process such personal data only when we need to, including:

- for the purpose of a product or service we provide to you with your explicit consent, cf. GDPR art. 6.1(a) and art. 9.2(a).
- We process special categories of data about you (membership of a trade union and health information) to give you certain discounts and other benefits with your consent, cf. GDPR, art. 6.1(a) and 9.2(a).
- for the purpose of assessing your financial situation in connection with a credit assessment, where budget information or other documents may reveal special categories of personal data, with your explicit consent, cf. GDPR art. 6.1(a) and 9.2(a).
- for the purpose of complying with a legal obligation to which we, as a financial institution, are subject, cf. GDPR art. 6.1(c) and art. 9.2(g).
- We process special categories of data about you (political standing) used in financial crime compliance area to investigate unusual activity based on legal requirements in the Danish Anti-Money Laundering Act (*Hvidvaskloven*), cf. GDPR art. 6.1(c), 9.2(g) and 9.3.
- We may process special categories of data about you in whistle blower cases subject to special requirements and protection under the Whistle Blower Act, cf. GDPR art. 6.1(c), 9.2(g) and 9.3.
- We may process special categories of personal data about you if such processing is necessary for the establishment, exercise or defence of legal claims, cf. GDPR art. 6.1(f) and art. 9.2(f).

6. How do we collect the information we have about you?

Personal data collected from you

We collect information directly from you or by observing your actions, including when you

- fill in applications and other forms for ordering products and services.
- provide us with your household information.
- submit specific documents to us.
- participate in meetings with us, for example with your adviser or as a representative of the business customer you are connected with.
- speak with us on the phone.
- use our website, our digital apps and solutions and products and services.
- participate in customer surveys or promotions organised by us.
- we track your subscription to newsletters.
- we collect personal data from electronic communications, telephone and video recordings in specific situations.
- Participate in social events organised or held by us.
- communicate with us by letter and digital means, including emails, online meetings or social media.

Recording and monitoring of electronic communications, including telephone conversations and online meetings

We may be obliged to monitor and store all electronic communications, including, for example, chat conversations, emails, online meetings or telephone conversations with you. We store this information for as long as we are legally required to do so.

Incoming and outgoing calls and online meetings may be recorded, listened to and stored in compliance with such regulatory requirements, but also for the purpose of documenting what was said, done and agreed. Visit our website to learn more about the [recording of conversations](#) and your rights in that regard.

To improve the quality of our meetings with you and provide a better customer experience, we may use your personal data to automatically transcribe online meetings,

and to take meeting summaries. We use AI technology for transcription and summarising meetings. The transcription will additionally be used to analyse and ensure the accuracy of the summaries. Read more about how we process your personal data in our information on [automatic transcription and meeting minutes](#).

Cookies

We use cookies on our websites and in our digital solutions and apps. When you first enter one of our websites or download our apps, we set the cookies that are necessary to enable you to use our services (strictly necessary cookies). If you consent to additional cookies, such as functional, statistical and/or marketing cookies, we set cookies according to your choices to measure, analyse and improve the use and performance of our products and services and to send you relevant marketing messages.

Some marketing cookies are owned by third parties. Depending on the situation, we may either share responsibility (joint data controllership) with these third parties for the processing of your personal information, or the third parties may process data on our behalf. In some cases, the third parties may also use the collected data for their own purposes in accordance with their own privacy policies. Further information about the various third parties can be found in our cookie policy [cookie policy](#).

Personal data collected from third parties

We receive and collect data from third parties, including from the following:

- If you have taken out a loan jointly with another person, we may collect information about you and your joint loan/credit account from the other borrower.
- The Danish Central Office of Civil Registration (CPR) or equivalent local central civil registration offices as well as other publicly accessible sources and registers. We process the data, for example for identification and verification purposes, and to check data accuracy, cf. section 11 of the Danish Data Protection Act and section 43 b of the Danish Financial Business Act.

- Our business customer with whom you are connected or associated with.
- Credit information agencies and warning registers. We process the data to perform credit assessments. We update the data regularly.
- Other entities of the Danske Bank Group if we have your consent, for example to provide you with better customised products and services.
- Other entities of the Danske Bank Group if applicable law allows or requires us to share the information, for example
 - i. if it is necessary for group-based administrative purposes or for compliance with control and/or reporting requirements established by the Capital Requirements Regulation, or
 - ii. for sharing suspicious activity reports with the Danish Special Crime Unit (NSK) in accordance with the Danish Anti-Money Laundering Act.
- External data processors such as business or other partners, including other banks, mortgage credit institutions and vendors, if we have your consent to this or if permitted under applicable law, for example
 - i. to provide you or our business customer with a service or product provided by an external business partner at your request
 - ii. when we register a mortgage, and therefore disclose information that is necessary to identify you and to perform our agreement with you, or
 - iii. to prevent and detect money laundering, fraud, abuse and loss.
- Moreover, we may receive information from public authorities, including, for example, the Public Information Server (OIS) and the Danish Energy Agency regarding, for example, energy performance certificates, calculated carbon emissions, pollution levels, noise levels, radon classification, etc.

7. Third parties that we share your personal data with

We will keep your data confidential, but we may share it with the third parties listed below if disclosure and sharing of personal data are justified. These third parties are also required to keep your personal data secure and confidential.

- Other entities within the Danske Bank Group if we have your consent, for example to provide you with better customised products and services.
- Other entities within the Danske Bank Group if this is a condition for providing the financial services or products you have requested.
- Other entities within the Danske Bank Group or a third party, so that you can receive an offer for a product or service, where this has been agreed with the business customer to whom you are connected.
- Other entities within the Danske Bank Group if applicable law allows or requires us to share the data, for example if necessary for group-based administrative purposes or compliance with control and/or reporting requirements established by the Capital Requirements Regulation, or for sharing suspicious activity reports with the Danish Special Crime Unit (NSK) in accordance with the Danish Anti-Money Laundering Act.
- If you or the business customer to whom you are connected has, for example, asked us to register a mortgage deed or redeem a loan with another creditor, we will disclose the information necessary to identify you and to comply with the agreement.
- Generally, we perform our own property valuations, but we may request our business partners, including home a/s, to perform the valuation. For the purpose of contacting you or our business customer, and performing a valuation of your property, we disclose the following data: purpose of the valuation, name, address, telephone number, email address and relevant property data such as the records of the Danish Building and Housing Register (BBR), information registered in the land registry, etc.
- Guarantors, individuals holding a power of attorney, lawyers, accountants or others to whom you or our business customer has authorised us to disclose the information.

- If you have taken out a loan jointly with another person, we may share your information with the other borrower.
- External business partners, data processors, including other banks, mortgage credit institutions and vendors, if we have your consent to this, or if this is permitted under applicable law. We share this information, among other things, to be able to offer you a loan, register a mortgage or redeem a loan provided by an external partner, at your request, or to prevent and detect money laundering, fraud, abuse and loss.
- Lawyers, accountants and consultants.
- Courier services. We may use courier services to deliver, for example, loan documents to you, and we disclose your name, address and telephone number to them, so you can receive the documents.
- Data processors, including Danske Bank, for example in connection with procuring documentation in accordance with anti-money laundering legislation, and IT service providers, in countries outside the EU/EEA.
- Social media companies, such as Meta and Google, when you have given consent to marketing cookies.
- Public authorities as required by applicable law or according to court orders or requests ½ from the police, the bailiff or other authorities. This could include the Danish Special Crime Unit (NSK) in accordance with the Danish Anti-Money Laundering Act, the Danish tax authorities in accordance with the Danish Tax Reporting Act and the Danish central bank (*Danmarks Nationalbank*) for statistical and other purposes.
- Regulators, such as the Danish Financial Supervisory Authority (*Finanstilsynet*), the Danish Data Protection Agency (*Datatilsynet*), the Danish Agency for Digital Government (*Digitaliseringsstyrelsen*), Danish law enforcement agencies and authorities in Denmark and other countries, including countries outside the EU/EEA, in connection with their duties.
- Credit information agencies. If you default on your obligations to Realkredit Danmark and/or Danske Bank, we may report you or our business customer to the credit information agencies and/or warning registers in accordance with applicable law.

- Debt collection agencies for debt collection purposes. In the event of breach or default, we will share your personal data and information about your debts with a debt collection agency.
- In connection with transactions (including transfers, asset sales, mergers and acquisitions) which entail transfer of all or part of your business to another company, we may share your personal data to the extent necessary to complete the transfer and your customer relationship within the framework of the legal requirements we must comply with.
- Our business customer, if you are employed by that customer.

8. Use of Artificial Intelligence (AI), Profiling and automated decision-making

AI systems we use

We use AI systems that analyse patterns in data and generate predictions, recommendations and decisions to improve our services and protect our customers. By AI systems, we mean systems that, based on input, generate output – such as predictions, recommendations or decisions with a degree of autonomy. We also use rule-based automated processes that do not constitute AI in this sense.

We may use such systems for the following purposes, on the legal bases set out below:

- Credit assessment and lending decisions, where the system analyses financial and other relevant data, such as your income, expenses and payment history, to assess your creditworthiness and the likelihood of default and to support decisions concerning the loan products and loan amounts we can offer you. We process the data because this is necessary to take steps before entering into an agreement with you or to perform our agreement with you, cf. GDPR art. 6.1(b).
- Prevention and detection of fraud, money laundering and other financial crime, where the system analyses customer data and patterns to identify unusual or suspicious activity and support our financial crime prevention and compliance processes. We process the data to comply with legal obligations under applicable

financial crime legislation, including the Danish Anti-Money Laundering Act (Hvidvaskloven), and based on our legitimate interests in protecting our customers and our business against fraud and other financial crime, cf. GDPR art. 6.1(c) and 6.1(f).

- Risk assessment and monitoring, including the use of AI-assisted tools to scan customer data for early signs of financial weakness. Carried out in compliance with regulatory obligations, cf. GDPR, art. 6.1(c).
- Personalisation and direct marketing, the system generates recommendations about products and communications tailored to your profile in order to provide you with relevant offers and improve the efficiency of our customer communications. Your consent or legitimate interest in ensuring that marketing efforts are relevant and targeted to reduce unnecessary communications, cf. GDPR, art. 6.1(a) and GDPR, art. 6.1(f).
- Automatic transcription and summarisation of customer meetings to enhance meeting quality and improve the customer experience. Transcription may also be used for internal meetings and external meetings with suppliers and partners for the purpose of ensuring documentation of what has been said, done and agreed during these meetings, cf. GDPR, art. 6.1(b) and art. 6.1(f) and the description under [automatic transcription and meeting minutes](#).
- Processing of applications and supporting documents, where we use AI-based tools to read and extract relevant information from applications, budget information and other documents relating to your application, loan or other products and services. We use the information to process your application and administer your products and services efficiently and accurately. We process the data because this is necessary to take steps before entering into an agreement with you or to perform our agreement with you, cf. GDPR art. 6.1(b), or based on our legitimate interests in ensuring efficient and accurate administration, cf. GDPR art. 6.1(f).
- Improvement and development of products and services – we develop, test and improve our products, services and internal processes, using aggregated, anonymised or pseudonymised customer data where

possible. Legitimate interest in improving and securing our services, cf. GDPR, art. 6.1(f).

- Development, training and improvement of internal risk and analytical models, where we use customer data to develop, train, test and improve models used for purposes such as credit assessment, credit risk monitoring, Internal Ratings-Based (IRB) modelling, fraud detection and prevention of money laundering. The models are used by Realkredit Danmark and other entities within the Danske Bank Group for relevant risk management and compliance purposes. Customer data is not used to train general-purpose AI or large language models (LLMs). Where possible, we use anonymised or pseudonymised data. Depending on the purpose, we process the data to comply with our legal obligations, cf. GDPR art. 6.1(c), or based on our legitimate interests in maintaining accurate and effective models for risk management, regulatory compliance and the protection of our customers and business, cf. GDPR art. 6.1(f).

Profiling

We are constantly working to develop, improve and manage our products and systems. We use data analysis and statistics and evaluate our analyses, models and theories on customer behaviour with the use of advanced, innovative analytical methods, such as machine learning and AI. For example, this helps us to set fees and prices, perform credit assessments, prevent money laundering, prevent and detect fraud, assess the likelihood of default and value assets, and provides the basis for our marketing and business development. We continually process customer personal data, develop profiles with the use of machine learning models to help us to offer products that meet our customer's unique needs and prioritise customer enquiries in an efficient way. We also process personal data for process and system development and improvement purposes, including through tests.

We may use automated processing tools, including AI-powered solutions, to improve the efficiency of our services. These tools are subject to appropriate safeguards and human oversight. Personal data processed through

these tools remains subject to the same protection standards as all other processing activities.

We use behavioural and demographic personal data for statistical analysis and for developing new models, products and services. We analyse both publicly available data, internal data, including data from other entities of the Danske Bank Group, and external data. The analyses allow us to create customer profiles and capture life-changing events, such as first job, home purchase or retirement. We do this to be relevant to our customers and to provide the best financial advice. Our processing of personal data for the above-mentioned purposes is always based on an appropriate legal basis, such as your consent, and you will be informed in more detail when we use your personal data in such a process.

As part of our profiling activities, we use cookies and similar technology on our websites and in our digital apps to build and refine customer profiles for marketing purposes, including marketing through digital channels and social platforms such as Meta. You can read more about this in our [cookie policy](#).

We also use profiling and data modelling to assess the environmental, social and governance (ESG) risk of the sole proprietorship and our business customers.

You have the right at any time to object to the processing of your personal data for direct marketing purposes, including profiling carried out in connection with such purposes. Please see section 11 for information on how to exercise this right.

Automated decision-making

When using automated decision-making, we use our systems to make decisions without human involvement based on the data we have about you. Depending on the specific decision, we also use personal information from public registers and other public sources. Automated decision-making helps us ensure that decisions are quicker and more fair, efficient and correct than decisions made through a similar manual process.

When we use automated decision-making, you will receive additional information on the decision-making basis and the significance and the envisaged consequences for you. You can always express your point of view as regards

a decision that is solely based on automated processing if the decision produces legal effects for you (such as the cancellation of an agreement) or in similar ways has major consequences for you (such as the refusal of a loan), and you have the right to obtain human intervention in the decision (such as an employee reviewing an application that is solely based on algorithms).

Examples of automated decision-making:

- In relation to loans, we consider information about your income, your expenses and how well you have kept up on payments in the past. This will be used to determine the amount of money we can lend you.
- In relation to loans to business customers, we assess the business customer's financial statements and review whether payments have previously been met. We use this to determine the amount we can lend to the business customer.
- In relation to the prevention and detection of money laundering, we perform identity and address checks against public registers as well as sanctions checks.
- In relation to the prevention and detection of fraud, we do our utmost to protect you and our business customer from criminal or fraudulent activities.

See section 11 'Your rights' for more information on your rights in relation to automated decisions.

9. Transfer of 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 and Microsoft, for the provision of agreed services to the Danske Bank Group. With the supplementary measures we have implemented, we maintain a level of protection equivalent to the requirements of the GDPR, without the recipient country's legislation undermining it.

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. You can read more about how we transfer personal data here: [Transfer of your data to third countries website](#).

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

We keep your personal data for as long as it is needed for the specified purpose(s) for which your personal data was collected, or as required by law. The personal data will subsequently be deleted or anonymised. Below you will see examples of retention periods, but please note that the list is not exhaustive.

Examples of retention periods:

- If you, as a potential customer, have asked for a loan calculation or an offer for a loan, but decline the offer and therefore do not become a customer with us, your

personal data will normally be stored for six months, but may for some purposes be stored longer to comply with legal obligations, for example under the Danish Anti-Money Laundering Act.

- If you have requested an offer for a loan or other product or other payment on behalf of a potential business customer, your personal data will normally be stored for 6 months even if no customer relationship has been established; however, it may for some reasons be stored longer to with legal obligation, for example under the Danish Anti-Money Laundering Act.
- When your customer relationship with us ends, or when the customer relationship with the business customer to whom you are connected or associated with ends, we normally retain your personal data for a further 5 years. This is primarily to meet our obligations under the Danish Bookkeeping Act, the Anti-Money Laundering Act and requirements set by the Danish Financial Supervisory Authority.
- In certain circumstances, we keep your information for a longer period of time. For example, this applies to information on credit and collateral for up to 10 years after expiry to document our agreement for establishing, exercising or defending of a legal claim. In that case, we may keep your data for up to 10 years with the addition of a reasonable administrative case management buffer should a claim or matter arise at the end of the limitation period.
- In one circumstance, we keep your personal data for a period 30 years or more based on legitimate interest, cf. GDPR art. 6.1(f). This is exclusively for use in our Internal Ratings Based (IRB) models used for Danske Bank's risk management and calculation of capital requirements under the Capital Requirements Regulation (CRR) and where we are required to document financial crises cycles.
- We keep your voice recordings for 15 months for general documentation purposes, and if the voice recording relates to investments, we have a legal obligation to keep it for 5 years under MiFID II. Reference is made to our information on [recording of conversations and](#)

[online meetings](#) for details on our recording and processing of personal data in relation to conversations and online meeting recordings.

- We retain transcriptions of online meetings with customers for 30 days for analysis and to ensure the accuracy of the minutes based on these transcriptions. The transcription of internal meetings and external meetings with suppliers and partners will be retained for as long as necessary to fulfil the purpose for which they are created, cf. [Automatic transcription and meeting minutes](#).
- Consent to the use of cookies on our website is stored for a period of one year unless withdrawn by you at an earlier date.
- Surveillance videos are deleted 30 days after they were made in accordance with the Danish TV Surveillance Act (TV-overvågningsloven). In case of a police investigation, the video may be stored for a longer period.

11. Your rights

When personal data about you is processed, you have various rights. These rights are described in this section. To exercise your rights, you can, for example

1. contact us on our main telephone number +45 70 15 15 16
2. contact your adviser (if you have one)
3. contact us at GDPR-insight@rd.dk.

See section 13 for more information on how to contact Realkredit Danmark.

Right of access to your personal data

You have the right to request access to your personal data and to request information about the processing we carry out. 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 against 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

If you wish to exercise your right of access under the GDPR, you can contact us at GDPR-insight@rd.dk, submit the request via [website form](#) or via your adviser (if you have one).

Rights related to automated decision-making

When we use automated decision-making in our processes, you will always be notified separately about our legal basis for this and your option to be excluded from automated decision-making. Furthermore, you will be informed about the reasoning behind the automated decision-making, and you will be given the opportunity to express your points of view and to object to the decision. You will also be informed of your right to request a manual review of any automated decision.

Right to object

In certain circumstances, you have the right to object to the processing of your personal data, for example when we use automated decision-making processes, or when the processing is based on our legitimate interests.

Objection to direct marketing

You have the right to object to our use of your personal information for direct marketing purposes, including profiling related to such purpose.

Right to rectification of your data

If your personal data is inaccurate, you are entitled to have your data rectified. If your personal data is incomplete, you are entitled to have the personal data completed, including by providing us with supplementary information.

Right to erasure ('right to be forgotten')

You are entitled to have your personal data erased if the personal data is no longer necessary for 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 example if we are obliged by law to hold your data for a certain period of time, for example as stipulated in the Danish Anti-Money Laundering Act or the Danish Bookkeeping Act. In such situations, we cannot erase your data until the retention period has expired.
- For the performance of a task carried out in the public interest, such as sending statistical data to the Danish Nationalbank.
- For establishment, exercise or defence of legal claims.

Right to restriction of processing

If you believe that the data we have registered about you is incorrect, or if you have objected to our use of the data, you are entitled to have the use of your personal data restricted to storage only until we can verify the correctness of the data or check if our legitimate interests outweigh your interests.

If you are entitled to have the personal data we have registered about you erased, but it is required by you to defend a legal claim, you may also request us to restrict the use of the data to storage.

If we need to use the data solely to assert a legal claim, you may also demand that other use of the data be restricted to storage. We may, however, be entitled to use the data for other purposes, for example to assert a legal claim or if you have consented to this.

Withdrawal of consent

If consent is the legal basis for a specific processing activity, you can withdraw your consent at any time by contacting us (see sections 11 and 13). Please note that if you withdraw your consent, we may not be able to offer you certain services or products. Please also note that we will continue to process your previously collected personal data, for example to fulfil an agreement we have made with you or if we are required by law to do so.

Sometimes consent is given for only one specific processing purpose (one-time consent), such as a consent to sharing personal data with a third party. Withdrawal of a one-time consent will not have any legal effect due its one-off nature.

Right to data portability

You have the right to receive personal data which you have provided to us and which is processed by us digitally in a structured, commonly used and machine-readable format. You also have the right to request that we transmit this data directly to another data controller.

12. Changes to this privacy notice

We may change or update this privacy notice on a regular basis. In case of changes, the 'effective from' date at the top of this document will be changed. 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.

13. Contact details and how to complain

You are always welcome to contact us if you have questions about your rights or how we process personal data. You can contact us as follows:

1. Call our main telephone number +45 70 15 15 16
2. Contact your adviser directly (if you have one)
3. Send a letter to:

Realkredit Danmark A/S
Bernstorffsgade 40
DK-1577 København V

If you wish to exercise your rights under the GDPR, you can contact us at GDPR-insight@rd.dk or via your adviser (if you have one).

Data protection officer

You can contact our data protection officer with all questions on our use of your personal data by sending an email to dpofunction@rd.dk or a letter to Realkredit Danmark:

DPO of Realkredit Danmark A/S
Bernstorffsgade 40
DK-1577 København V

Complaints

If you are dissatisfied with how we process your personal data or if your dialogue with our data protection officer has not led to a satisfactory outcome, you can lodge a complaint with our complaints handling unit:

Realkredit Danmark A/S, Legal
Bernstorffsgade 40
DK-1577 København V
Email address: legal@rd.dk

You can also lodge a complaint with the Danish Data Protection Agency:

The Danish Data Protection Agency
Carl Jacobsens Vej 35
DK-2500 Valby
Email address: dt@datatilsynet.dk

If your residence or the place of the alleged infringement is in or is related to another member state than Denmark, you can typically also lodge a complaint with the data protection authority in that member state. You always have the option to try your case in court.