Danica's privacy notice for personal customers and private individuals (Denmark)

Danica

Effective from 11 November 2026

Introduction

This privacy notice sets out how Danica processes your personal data.

Danica is the data controller for the processing of the personal data described in this privacy notice. Contact details:

Danica Pension, Livsforsikringsaktieselskab, company reg. (CVR) no. 24256146, Bernstorffsgade 40, DK-1577 København V.

This privacy notice applies to personal customers, potential personal customers, related parties, policyholders and beneficiaries with Danica as well as to sole traders, agents, corporate decision-makers and other private individuals with whom we interact or collaborate.

1. What personal data do we process?

Depending on the services or products you order, receive or are interested in, we process different kinds of personal data, including

- contact information, civil registration (CPR) numbers and similar basic information
- information about your profession, job and education
- information about your employer if your scheme is a company pension scheme
- financial information, for example your annual salary, amount of pension contribution and personal tax information.
- information about your family and household who are typically designated as beneficiary(ies) or insured
- proof of identity, for example photocopies of your passport, driver's licence and health card
- digital information related to your use of our websites, platforms and digital applications, including traffic data, location data, behavioural data and other communication data, e.g. by using cookies and similar technology
- details about the products and services we provide to you, including how you use them and your preferences towards them
- health information, including medical certificates and medical records
- information about your visits to our offices, including video surveillance
- recordings of phone conversations with you, as well as transcripts and summaries of your conversations during online meetings prepared using AI technology, read more here

2. What we use your personal data for

We process your personal data for the purpose of providing our products, i.e. pension schemes and insurance covers.

We also process your personal data for the following purposes:

- Making offers
- Customer service, advice and administration of your pension covers, insurance policies and healthcare products
- Preparation of financial statements
- Ensuring correct payment of pension contributions from employer
- Handling complaints
- Identification and verification in accordance with the Danish Anti-Money Laundering Act as well as prevention and detection of money laundering
- Setting prices and fees
- Risk management
- Development and administration of our products and services, systems and business. We process personal data for the development, testing and maintenance of systems and solutions using artificial intelligence, including machine learning.

This supports our work when we need to search for specific information in large data volumes, summarise, analyse, process or improve text and layout in data sets, documents, letters, and other communication.

In addition, generative artificial intelligence is used for the personal productivity and efficiency of employees, including to summarise, analyse and improve text and content, and to find specific information in large volumes of data.

In certain cases, we use machine learning to assess the risk of long-term sick leave in order to contact you with an offer

of early preventive support or help finding the right treatment.

• Protecting you and Danica against fraud and ensuring that our customers will not be charged higher premiums due to insurance fraud. On suspicion of fraud, we may under special circumstances initiate an observation procedure using the necessary human and technical resources. Further, prior to any observation we may conduct a location check. This involves familiarizing ourselves with the physical conditions around relevant locations, such as a residence or workplace, and vehicles. In connection with this, we will observe the insurance industry's code on investigation of suspected insurance fraud cases and any relevant legislation.

• Complying with legal requirements, e.g. reporting to SKAT and the Danish Financial Supervisory Authority

• Checking, testing and monitoring our compliance with internal policies and rules, regulatory and legislative requirements, e.g. in relation to data protection

• Physical security, including the use of video surveillance of building facades, entrances to our other premises, reception, etc.

• 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 such marketing by law

• Allowing Danica or third parties to pursue statistical, scientific and research purposes as part of research projects or similar. For such purposes, personal data will to the extent possible be pseudonymised

• If you are an administrator, decision-maker or other contact person with a company with which we have entered into an agreement, we will process your personal data for purposes of managing the contract with the company, granting you administrator rights and otherwise nurturing the customer relationship

• If you are a policyholder or beneficiary of a scheme, we will process your data for purposes of managing the insurance policy or scheme and ensuring proper administration, handling and payout

Cookies

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

Some of the marketing cookies that Danica uses are owned by third parties, e.g. Facebook or Google. We continue to be responsible for third party use of data that is processed for our purposes (shared data controllership). We refer to our cookie policy for further information.

3. What is our legal basis for processing your "ordinary" personal data, CPR number and information about criminal offences?

We must have a legal basis (lawful reason) to process your "general" personal data, i.e. any data which is not "sensitive". The legal basis will be one of the following:

• You have given us consent to process your personal data for a specific purpose, cf. the General Data Protection Regulation (GDPR), art. 6.1(a)

• You have entered into, or you are considering entering into an agreement with us on a service or product, cf. the GDPR, art. 6.1(b)

• To comply with a legal obligation, cf. the GDPR, art. 6.1(c), for example under

– the Danish Tax Control Act (*skattekontrolloven*)

– the Danish Bookkeeping Act (*bogføringsloven*)

– the Danish Insurance Business Act (*lov om forsikringsvirksomhed*)

– the Danish Data Protection Act (*databeskyttelsesloven*) (§ 11(2) regarding the processing of your CPR number) and the Danish Insurance Business Act § 69.

– the Danish Insurance Contracts Act (*forsikringsaftaleloven*)

– the Danish Anti-Money Laundering Act (*hvidvaskloven*)

– the Danish CPR Act *(CPR-loven)*

– the EU Market Abuse Regulation (MAR)

• To ensure an adequate level of IT security, cf. the GDPR, art. 6.1(c), cf. art. 32.

• It is necessary to pursue a legitimate interest of Danica, cf. the GDPR. art. 6.1(f). For example, this may be to prevent abuse and loss, for documentation and security purposes, for direct marketing purposes or to comply with the Danish Act on CCTV Monitoring. We will do so only if our legitimate interest in each case is not overridden by your interests or rights and freedoms.

• Information about criminal offences, cf. the Danish Data Protection Act 8.3 and 8.5.

4. Sensitive personal data

Part of the data we hold about you is sensitive.

Types of sensitive personal data
We process the following types of sensitive personal data:

- Trade union membership information
- Information about your health, including any health information you have provided to us or we have obtained from healthcare professionals based on your consent

Purposes of processing sensitive personal data
We will process sensitive personal data only when we need to, including

- for the purpose of a product or service we provide to you, including to make a health assessment, treat your injury or illness and to pay out loss of earning capacity benefits
- for the purpose of complying with any agreements related to your trade union membership
- calculations and analyses made by the actuarial department, risk management and, in some cases, correction of errors and testing of systems

- for the purpose of complying with legal requirements that apply to us as a financial institution

Legal basis for processing sensitive personal data
We may process sensitive personal data about you on the legal basis of

- as regards trade union membership, the Danish Data Protection Act, s. 12, and the GDPR, art. 6.1(b) and art. 9.2(b)
- establishment, exercise or defence of legal claims, cf. the GDPR, art 6.1(f) as well as 9.2(f)
- To test output from IT applications, cf. GDPR Art. 6.1(c) and 9.2(g), cf. Art. 25.1, cf. 5.1a and 5.1.d.

5. How do we collect data about you?

Personal data received from you
We receive data directly from you when you, for example

• fill out applications and other forms for ordering products and services

• submit specific documents to us

• talk to us on the phone (see more on recording of phone conversations below)

• use our website, mobile applications, products and services

• participate in customer surveys or promotions organised by us

• communicate with us via letter or digital means, including emails, social media, etc.

Personal data which we collect or receive from third parties

We register and use personal data about you received from third parties, such as

• the Danish Central Office of Civil Registration (CPR no.) and other publicly accessible sources and registers. We process the data, for example for identification and verification purposes and to check data accuracy, cf. the Danish Data Protection Act, s. 11

• publicly available sources, e.g. the internet, including data from open social media and financial information (e.g. from CVR.dk and BiQ) in connection with anti-money laundering activities and suspicion of fraud

• CVR.dk and BiQ in connection with applications for payout due to reduced earning capacity and cases where benefits are paid out due to reduced earning capacity, because the information registered with CVR.dk and BIQ may be relevant to the earning capacity assessment

• healthcare professionals, for example doctors, hospitals and clinics (if you have consented to the healthcare professional's disclosure of data to Danica, cf. the Danish Health Care Act (*sundhedsloven*), s. 43)

• your employer or broker, who discloses certain information in connection with an offer or administration of your schemes, for example

• the policyholder (our customer) when you are designated as beneficiary of a scheme, advice is requested for an entire household, or similar

• other pension and insurance companies and banks

• SKAT, which may disclose tax information

• municipalities and other public authorities and bodies

• the Danish Centre of Health & Insurance

• geomatics witch estimates income and wealth etc. for people of the same age and residential area

• entities of the Danske Bank Group, for example to provide you with better customised products and services (if we have your Group consent)

• other entities of the Danske Bank Group if applicable legislation allows or requires us to share the data, for example if it is necessary for group-based management purposes or compliance with control and/or reporting requirements established by law, or the sharing of notifications to the Danish Special Crime Unit (NSK) in accordance with the Danish Anti-Money Laundering Act.

6. Third parties with whom we share your personal data

We will keep your data confidential. However, in some instances we may share your personal data with third parties if required. Such third parties are also required to keep your personal data secure and confidential. The categories of third parties to whom we disclose personal data and the categories of personal data are set out below:

Reinsurance companies
Purpose of processing:
The data is used for calculation of risk etc. to allow Danica Pension to take out reinsurance.

Categories of personal data:
Personal data

- General client information (gender, age, client name)
- General insurance information (policy number, claim number)
- Health information (description of treatment, description of diagnose, information regarding provider and their speciality)
- Savings data
- Capital at risk

Broker
Purpose of processing:
The broker requires information for putting pension schemes out to tender and serving customers of broker-serviced pension schemes.

Categories of personal data:
Personal data

- Amount (the amount the employee contributes to the pension scheme)
- Company reg. (CVR) no. (relevant for sole traders)
- Email

- Information about employer
- Employee group (salaried employees, management, etc.)
- Insurance cover
- Investment profile
- Name
- Pension information from other providers
- Telephone number
- Position / job title
- Pension savings
- Signature (physical or MitID)
- Work description
- Policy number
- Salary information

Confidential personal data

- CPR number

Auditors (Accountants)
Purpose of processing:
The purpose of the processing is to advise customers and to have the required audit performed

Categories of personal data:
Personal data

- Amount (the amount the customer contributes to the pension scheme)
- Annual tax report (21A cases (cases of excessive contributions to annuity pensions where funds are to be transferred to life annuity))
- CVR number
- Tax information
- Company pension agreement
- Information about employer
- Any information necessary for the auditors to fulfil their obligation as auditors

Lawyers
Purpose of processing:
If Danica needs to defend itself against a legal claim or obtain external legal advice.

Categories of personal data:
Personal data

All personal data required to provide advice in a pending case. This may potentially be any personal data, including contact information, information on pension and insurance products, pension savings, information about tax and personal finances and CPR number

Sensitive personal data

- Health information

Danske Bank (if Group consent is given)
Purpose of processing:
To offer you the best possible advice.

Categories of personal data:
Personal data

- Address
- Customer number
- Email
- Name
- Marital status
- Telephone number
- Company pension agreement
- Interest information
- Information on arrears, if any
- Salary information
- Tax information
- General information on income and assets

Confidential personal data

- CPR number

Pension and insurance providers
Purpose of processing:
Transfer of pension schemes and customer relationships to other providers

Categories of personal data:
Personal data

- Name
- Address
- Email
- Transfer of pensions between two pension providers
- Transfer of pensions between a pension provider and a bank
- Transfers of pensions from employees
- Registration of endorsement of a mortgagee's interest in policy
- Obtaining FP certificates
- Annual tax report
- Information about employer
- Position / job title
- Salary information

Confidential personal data

- CPR number

Sensitive personal data

- Health information

Employer
Purpose of processing:
To ensure correct payment of pension contributions from employer and the employer's handling of sickness, injuries, reduced working hours, etc.

Categories of personal data:
Personal data

- Customer number
- Name
- Address
- Email
- Telephone number
- Company pension agreement

- Marital status
- Age
- Agreement no.
- Date of birth
- Employee group
- Form of employment
- Gender
- Signature (physical or MitID)
- Work description
- Salary information
- First day of sickness absence

Confidential personal data
- CPR number
- Number of hours the person is able to work relative to normal working hours

Sensitive personal data
- Generally, no sensitive personal data is disclosed.

Danish Financial Supervisory Authority (the FSA) – reporting under the Market Abuse Regulation (MAR) and Fit & Proper
Purpose of processing:
The purpose of the processing is to submit statutory reporting to the FSA and to perform Fit & Proper assessments.

Categories of personal data:
Personal data

- Any information required to answer FSA requests for clarification, except health information
- It should be noted that the FSA seldom processes cases relating to private individuals

Probate court
Purpose of processing:
Personal data is processed when the probate court determines how an estate is to be administered.

Categories of personal data:
Personal data

- *About the deceased (the policyholder)*
  - Name
  - Policy number
  - Date of death
  - Information on cover
  - Property tax levied on the estate

Confidential personal data
- CPR number

- *In the event of beneficiary designation, we will provide information (on the beneficiary)*
  - Name
  - Address
  - Kinship
  - Date of birth

Danish Insurance Complaints Board
Purpose of processing:
The purpose of the processing to handle complaints.

Categories of personal data:
Personal data

- Name
- Address
- Telephone number
- Policy number
- Claim number
- Other information considered to be of relevance to the complaint

Confidential personal data
- CPR number

Sensitive personal data
The case files of some complaints – e.g. involving personal injury – will also include health information. Moreover, the case files of some complaints may include information about criminal offences, cf. the Danish Data Protection Act, s. 8.

Danish Special Crime Unit (NSK)
Purpose of processing:
The purpose of the processing is to identify any cases of actual or suspected money laundering.

Categories of personal data:
Personal data

- Any information required to clarify cases of money laundering, but never health information

Danish Centre of Health & Insurance (Health & Insurance)
Purpose of processing:
The purpose of the processing of personal data is to ensure that as many individuals as possible with health issues may be offered life or pension insurance at terms based on adequate medical and statistical information.

Categories of personal data:
Personal data

- Name
- Address
- Email
- Age
- Job description
- Position
- Anticipatory pension

Confidential personal data
- CPR number

Sensitive personal data
- Health information
- Vocational rehabilitation
- Disability benefits

Hospitals and private clinics
Purpose of processing:
The purpose of processing is to ensure proper and correct treatment of customers in connection with treatment.

Categories of personal data:
Personal data

- File number
- Customer number
- Date of sick leave
- Email
- Information about employer
- Name
- Policy number
- Telephone number
- Position
- Date of injury

Confidential personal data
- CPR number

Sensitive personal data

- Health information

Municipalities
Purpose of processing:
The purpose of the processing is to ensure correct treatment of the data subject as regards referrals for treatment and benefits.

Categories of personal data:
Personal data

- Name
- Address
- Email
- Telephone number
- Date of sick leave
- Date of reactivation
- Information about employer
- Public benefits and services
- Effective date of termination of employment

Confidential personal data
- CPR number

Sensitive personal data
- Health information

Danish Central Office of Civil Registration (CPR)
Purpose of processing:
Keep information about residence etc. up-to-date through subscription to the civil register.

Confidential personal data
- CPR number

NemKonto system
Purpose of processing:
The purpose of the processing is to ensure that benefits are paid out to the right person.

Categories of personal data:
Personal data
- NemKonto account no.

Confidential personal data
- CPR number

SKAT (the Danish tax authorities)
Purpose of processing:
The purpose of the processing is to ensure payment of correct taxes.

Categories of personal data:
Personal data
- Policy number
- Pension savings
- Exempt value
- Effective date of agreement
- Contributions in the current year

Confidential personal data
- CPR number

In addition, we may obtain your tax information for the purpose of assessing your right to receive benefits in the event of loss of earning capacity.

Research
Purpose of processing:
The purpose of the processing is to allow Danica Pension or third parties to pursue statistical, scientific and research purposes as part of research projects or similar.

Categories of personal data:
Personal data
- In this context, personal data will to the extent possible be pseudonymised
- All (pseudonymised) data of relevance to the research project

Making personal data available to data processors

We enter into data processing agreements with all companies that process personal data on our behalf. Our data processors act exclusively under our instructions and are not permitted to process personal data in any other way than as agreed with us. We use such data processors to perform assignments in relation to:

(1) software / portal solution

(2) technical solutions

(3) market research

(4) electronic exchange of data with business partners

(5) digital concept for use in performing manual processes

(6) administration and arrangement of group life agreements on behalf of Danica (including Forenede Gruppeliv)

(7) statistical analysis

(8) remote storage capacity and storage of records

(9) communication and referral platform in connection with health and other claims

(10) marketing

(11) IT services, including maintenance and software support

(12) facility management

and other providers with whom we collaborate to process your personal data.

7. Transfers outside the EU and the EEA and international organisations

In connection with IT development and IT support, we transfer personal data to the following companies located in countries outside the EU/the EEA. They are:

Infosys Limited
No. 44/97 A, 3rd cross
Electronic City
Hosur Road
Bangalore
560100, Karnataka
India
Registration number: 13115

Danske IT and Support Services India, Private Limited
Campus 5 B
RMZ Ecoworld
Bangalore
Karnataka 560103
India

Inscale Aisa Sdn Bhd
Level 12, Menara Binjai, Jalan Binjai, 50450 Kuala Lumpur, Federal Territory of Kuala Lumpur, Malaysia

Danica Pension also uses cloud services provided by Amazon Web Services (AWS) for certain anti-money laundering activities and Microsoft (Azure) for data storage purposes. Moreover, some of our data processors use cloud services provided by Microsoft and AWS to process personal data on our behalf. The data is stored in regions within the EU/the EEA only. However, if AWS or Microsoft is ordered to disclose information to the US in order to comply with a legal obligation according to law or an order by a US public authority, AWS and Microsoft may transfer the data to the US.

When your personal data is processed in countries outside the EU/the EEA, we ensure that your personal data and data protection rights are protected by way of appropriate means. In that connection, we ensure that there is a legal basis for transferring the data to countries outside the EU/the EEA:

- If we transfer your personal data to parties in countries where the European Commission has found that the country ensures an adequate level of protection, we rely on the adequacy decision of the European Commission

- If we transfer your personal data to parties in the USA, we may rely on the EU-US Data Privacy Framework

- If we transfer your personal data to other third countries, we rely on the standard contractual clauses (SCCs) of the European Commission

- We may also transfer your personal data to parties outside the EU/the EEA on the basis of the specific exemptions set out in the GDPR, art. 49, for example art. 49(1)(e), if the transfer is necessary for our establishment, exercise or defence of a legal claim

8. Profiling and automated decision-making

Profiling
Profiling is a form of automated processing of your personal data in order to evaluate certain personal aspects relating to you to analyse or predict aspects concerning, for example, your personal preferences, interests, reliability, behaviour and location.

We use profiling and data modelling to:

- be able to offer you specific services and products that meet your preferences
- prevent money laundering
- determine prices of certain services and products
- evaluate the likelihood of default risk
- assess the risk of long-term sick leave in order to make pre care calls to you with an offer of early preventive support or help finding the right treatment
- use the information for sales and marketing purposes.

Automated decision-making
Automated decisions are decisions made without the involvement of our employees (i.e. without human involvement).

For example, we use automated decision-making to establish your pension scheme and to grant treatments. Automated decision-making helps us make sure that our decisions are quick, fair, efficient and correct, based on the personal data we have.

In relation to the prevention and detection of money laundering, we perform identity and address checks against public registers and check PEPs (politically exposed persons) and sanctions lists.

If the automated decision leads to an unfavourable result for you, the decision will be subject to manual processing (i.e. your case will be handled by one of our employees). This also applies to the majority of our cases concerning the conclusion of agreements for insurance products. For a small part of these cases, however, the process of setting up – or refusing to provide – insurance products, such as loss of earning capacity cover, is fully automated.

You have certain rights relating to automated decision-making. Please see "Your rights" and "Automated decision-making" below.

9. Recording of phone conversations

Incoming and outgoing calls may be recorded and stored to document what was said, what happened, and what was agreed during the conversation. We refer to Recording of phone conversations for more details on our processing of personal data and your rights in that respect.

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

We store your personal data only for as long as it is needed for the purpose for which your data was processed.

This means that as a general rule we store your personal data for as long as we are providing a service or a product to you. When your customer relationship with us has ended, we store your personal data for another ten years. The storage

period complies with the principles of limitation under the Danish Statute of Limitations Act (*forældelsesloven*).

In certain circumstances, we store your data for a longer period of time:

We store personal data processed in connection with pre care calls for a period of one year for the purposes of evaluating and improving the process.

We store personal data provided in connection with an offer that was not accepted for a period of six months after the rejection/expiry of the offer.

We store personal data collected with a view to complying with the Danish Anti-Money Laundering Act for a period of five years after the customer relationship has ended.

Surveillance videos are deleted 30 days after they were made in accordance with applicable law. In certain circumstances, and in connection with a specific case, the data may be stored for a longer period.

Phone conversations are deleted after the period set out here.

11. Your rights

Your rights in relation to personal data are described below. To exercise your rights, you can contact us via the contact details set out below.

Right to access your personal data
You have the right to request access to the personal data we process and information about where it comes from and what we use it for. You can obtain information about how long we store your data and about who receives data about you, to the extent that we disclose data. Your right of access may, however, be restricted to protect other persons' privacy or for purposes of our business and practices. Your right of access may be restricted due to the prevention, investigation, detection or prosecution of criminal offences. Our know-how, business secrets as well as internal assessments and material may also be exempt from the right of access.

Rights related to automated decision-making
You have the right to obtain information on how an automated decision was made and the effects of the decision, you can express your point of view, you can object to the decision, and you can 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. This is the case, for example, 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 data for direct marketing purposes, including profiling that is related to such purpose.

Right to rectification of your personal data
If data is inaccurate, you have the right to have the data rectified. If data is incomplete, you have the right to have the data completed, including by means of providing us with a supplementary statement.

Right to erasure ('right to be forgotten')
You have the right to have your data erased, provided the data is no longer necessary in relation to the purposes for which it was collected.

However, in the following cases, we may be or are required to store your data:

- for compliance with a legal obligation, for example if we are obliged by law to store your data for a certain period of time, for example under the Danish Anti-Money Laundering Act or the Danish Bookkeeping Act. In such situations, we cannot erase your data until that time has passed
- for the performance of a task carried out in the public interest
- for establishment, exercise or defence of legal claims

Restriction of use
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 may demand that we restrict the use of the data to storage. Use will be restricted to storage only until the accuracy of the data can be established or it can be verified whether our legitimate interests override your interests.

If you are not entitled to have the data we have about you erased, you may instead request us to restrict the use of the data to storage. If we need to use your data solely to exercise 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 exercise a legal claim or if you have granted your consent to this.

Withdrawal of consent
Where your consent is the legal basis for a specific processing activity, you may withdraw your consent at any time with prospective effect. Please note, however, that if you withdraw your consent, we may not be able to offer you specific services or products. Please also note that we will continue to use your personal data, for example for the performance of an agreement we have made with you, or if we are required by law to do so.

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 the right to request a copy of the data you have provided in a digital machine-readable format.

12. Changes to this privacy notice

We may change or update this privacy notice on a regular basis. In case of a change, 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 can you complain

You are always welcome to contact us if you have questions about your rights and how we process your personal data.

You can contact us on our main telephone number +45 70 11 25 25 or by email at Write to us (secure connection).

If you wish to exercise your rights regarding your personal data, you are welcome to contact us at dpindsigt@danica.dk.

Data protection officer

If you have any questions for our data protection officer, you can contact the department responsible for data protection by email at dpindsigt@danica.dk.

Person in charge of complaints

If you are dissatisfied with how we register and use your personal data, and the dialogue with the Data Protection Officer has not led to a satisfactory outcome, you can contact our complaints handling unit via Ris, ros og klager (secure connection) or by writing to Danica Pension, Bernstorffsgade 40, DK-1577 København V.

You can also lodge a complaint with the Danish Data Protection Agency: Datatilsynet, Carl Jacobsens Vej 35, DK-2500 Valby, email: dt@datatilsynet.dk.

If, for example, 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 supervisory authority for data protection in that member state.