

# NemLog-in privacy policy

## Introduction

This privacy notice for NemLog-in describes how the Agency for Digital Government processes your personal data in relation to the use of NemLog-in services and your rights in that regard.

## 1. We are the data controller – how to contact us?

Agency for Digital Government is the data controller for the processing of your personal data. You will find our contact information below:

Agency for Digital Government  
Landgreven 4  
1301 Copenhagen K  
Denmark

Central Business Registration number: 34 05 11 78

Phone no.: +45 33 92 52 00

Email: [digst@digst.dk](mailto:digst@digst.dk)

## 2. Contact information of the Data Protection Officer

The Ministry of Digital Government and Gender Equality has appointed a Data Protection Officer who provides guidance on the data protection regulation within the area of the Ministry of Digital Government and Gender Equality. The task of the Data Protection Officer is to support the Ministry of Digital Government and Gender Equality's compliance with the rules on the processing of personal data.

The Data Protection Officer can guide you on your rights in relation to the processing of your personal data within the area of the Ministry of Digital Government and Gender Equality.

If you have questions about our processing of your personal data, you are always welcome to contact our Data Protection Officer. You can contact our Data Protection Officer in the following ways:

- Via Digital Post: Send the mail to the Agency for Digital Government in the Digital Post. Write 'Attention: Data Protection Officer' in the subject field.
- Via email: [dpo@digst.dk](mailto:dpo@digst.dk). If you wish to contact the Data Protection Officer via email, please refrain from providing your

civil registration number (CPR number) or other sensitive/confidential information.

- Via letter: Agency for Digital Government, Attention: Data Protection Officer, Landgreven 4, 1301 Copenhagen K, Denmark.

### **3. Purpose and legal basis of the processing of your personal data**

The purpose of the Agency for Digital Government's processing of your personal data is:

- To make NemLog-in available where users with MitID or another approved means of identification can use the services: Login and authentication, Digital Fuldmagt (Digital Power of Attorney), MitID Erhverv, and Digital Signing.
- The Agency for Digital Government processes your personal data for purposes related to administration, management and maintenance of NemLog-in, as well as improvement of support services.

The legal basis for our processing of your personal data is based on:

- The Law on MitID and NemLog-in (law no. 783 of May 4th, 2021, regarding MitID and NemLog-in, as amended by law no. 1559 of December 12th, 2023)
- The EU General Data Protection Regulation Article 6, para 1, litra e, related to the processing of ordinary personal data
- The Danish Data Protection Act § 11, para 1, litra 1, related to the processing of the Danish civil registration number (CPR number).

#### **3.1. NemLog-in provides the following services:**

##### **3.1.1 Log-in and authentication – MitID broker**

Log-in is the function that is shown in the internet browser when you wish to log in to a digital self-service solution connected to NemLog-in, such as borger.dk, sundhed.dk, and virk.dk.

##### **3.1.2 Digital Fuldmagt (Digital Power of Attorney)**

Digital Fuldmagt allows you to be represented by another person in a digital self-service solution. You can be represented by a private individual, a business user, or a company.

##### **3.1.3 Digital Signature**

Digital signature makes it possible for you as a citizen or business user to sign documents in public and private digital self-service solutions. The signing service contains a validation service which can be used to validate the validity of signatures and electronic seals.

### 3.1.4 MitID Erhverv – Business Administration

MitID Erhverv allows user organisations to administer their business users, issue means of identification and assign and manage rights and certificates for business users.

## 4. Categories of personal data

### 4.1 When using NemLog-in as a private user

We may process the following categories of personal data about you when you use NemLog-in as a private user:

#### 4.1.1 Personal data

- Full name
- Pseudonym
- Date of birth
- User IDs and unique identification numbers (UUID numbers, PIDnumbers etc.)
- Civil registration number (CPR-number) and status on civil registration
- Contact information
  - Address
- Information on one's affiliations with enterprises originating from the Central Business Register (CVR-registret)
- Technical information such as: IP-address, browser information and session information
- Risk data received from MitID:
  - Information on device location that was used to log in, new work information, and the information on the identity and their latest use
- Services connected to NemLog-in that you have logged into
- Issued certificates related to signing with MitID, fingerprints (hash values) of signed documents, and reference text for signing
- Content of documents validated with NemLog-in's validation service
- Assigned and granted digital powers of attorney in NemLog-in's Digital Fuldmagt solution

#### 4.1.2 Sensitive personal data

We may process the following sensitive personal data if they are included in documents that are uploaded for validation:

- Information on race or ethnic origin
- Information that indicates or may indicate political, religious or philosophical believes
- Information about the data subject's trade union membership
- Health information, including genetic data

- Biometric data for identification purposes
- Information about sexual matters
- Information about criminal offenses
- Information about deceased individuals

## 4.2 When using NemLog-in as a business user

We may process the following categories of personal data about you when you use NemLog-in as a business user:

### 4.2.1 Personal data

- Full name
- Pseudonym
- Date of birth
- User IDs and unique identification numbers (UUID numbers, PIDnumbers etc.)
- Civil registration numbers (CPR-number) and status on civil registration
- Contact information
  - Email address
  - Address
  - Telephone no.
- Affiliations with companies in the CVR register
- Technical information such as: IP address, browser information and session information
- Risk data received from MitID:
  - Information about the location of the log-in, the device used for log-in, network information, and details about the identity and recent usage
- Services connected to NemLog-in that you have logged into
- Rights assigned to business users
- Persistent certificates issued for business use
- Issued certificates related to signing with MitID, fingerprints (hash values) of signed documents, and reference text for signing
- Content of documents validated with NemLog-in's validation service
- Assigned and granted digital powers of attorney in NemLog-in's Digital Fuldmagt solution

### 4.2.2 Sensitive personal data

We may process the following sensitive personal data if it is included in digital powers of attorney, signatures, documents uploaded as proof of identity or authorisations, and documents uploaded for signature validation:

- Data revealing racial or ethnic origin

- Data revealing political opinions, religious or philosophical beliefs
- Data revealing the subject's trade union membership
- Data concerning health status, including genetic status
- Biometric data for identification purposes
- Data concerning a natural person's sex life or sexual orientation
- Data concerning criminal convictions and offences or related security measures
- Data of deceased persons

## 5. Recipients or categories of recipients

We disclose or make available your personal data to the following recipients:

- Service providers, NemLog-in brokers, and other parties connected to NemLog-in.
- Authorities connected to Digital Fuldmagt (Digital Power of Attorney) can access data about citizens' power of attorney relationships.
- The Danish Business Authority is our data processor when providing support and can access data about businesses and business users registered via MitID Erhverv in support cases.
- POSTNORD STRÅLFORS A/S processes your personal data when sending to Digital Fuldmagt (Digital Power of Attorney) for printing and transportation of postal mails.
- Nets DanID A/S and Aeven A/S act as data processors on behalf of the Agency for Digital Government and handle the specific processing of personal data in NemLog-in.

Disclosures are limited to the personal data necessary for the use of NemLog-in. NemLog-in, as a broker receives data about your MitID in the form of an authentication response when you use MitID to log in to digital self-service solutions.

The Agency for Digital Government may, in certain cases, be required to disclose to other public authorities. The disclosure will be limited to the personal data necessary for the exercise of official authority.

The Agency for Digital Government makes your personal data available to the agency's data processors that assist with the operation and administration of IT systems related to the NemLog-in solution.

The Agency for Digital Government discloses IP addresses, URLs of visited websites with timestamps (along with an associated IP address), geographic location based on IP address, and information about browser version/engine and operating system version/engine to Akamai

Italy (Akamai Technologies Italy) for Akamai's traffic and security analysis of traffic related to NemLog-in signing and validation services, with the aim of continuously improving their overall solution to prevent large-scale attacks on NemLog-in and for troubleshooting/support. This is done primarily to ensure that Akamai can deliver its service correctly.

## **6. Transfer to recipients in third countries, including international organisations**

In general, we do not transfer your personal data to recipients outside the EU and the EEA.

Please note that if you use MitID Erhverv or use NemLog-in as a broker in Greenland or the Faroe Islands, the Agency for Digital Government will ensure a basis for the transfer.

## **7. Where your personal data originates from**

NemLog-in receives personal data from MitID.

The personal data processed in Digital Fuldmagt (Digital Power of Attorney) and Digital Signature is received from MitID. Additional personal data is obtained directly from you if it is entered into the solutions or provided in the form of documents or other data.

Personal data processed in MitID Erhverv is recorded when the organisation you represent creates and assigns business identities with rights to various digital self-service solutions and possibly links a dedicated authenticator.

## **8. Storage of your personal data**

The Agency for Digital Government stores your personal data for as long as is necessary in relation to fulfilling the purpose of administration and use of NemLog-in for users with MitID or MitID Erhverv.

## **9. Processing of personal data for providing support of NemLog-in**

The Agency for Digital Government also acts as the data controller regarding any personal data processed about you if you contact NemLog-in Support. NemLog-in Support helps users find information about NemLog-in and how to use the NemLog-in solution. With NemLog-in Support, users can receive help via phone, email and screen sharing.

The purpose of The Agency for Digital Government's processing of personal data when users contact NemLog-in Support is:

The provision of support in relation to the use of NemLog-in and NemLog-in's service areas, as well as improvement of support services.

The legal basis for our processing of your personal data is based on:

- The legal basis for our processing of your data in relation to inquiries via phone, email or live chat is based on the EU General Data Protection Regulation Article 6, paragraph 1, litra e, related to the processing of ordinary personal data in the exercise of official authority.
- The legal basis for processing your personal data in relation to the customer satisfaction survey, including the anonymised survey of trends in the phone calls, screen sharing and/or phone recordings follows Article 6 of the Data Protection Regulation, paragraph 1, litra a, on consent.
- The legal basis for our processing of your data, if you enter your civil registration number (CPR number) into the support's phone menu, is section 11 of the Data Protection Act, paragraph 1, for processing of CPR.

In relation to screen sharing, the supporter will be able to see the personal information that may appear on the page where you need support.

In relation to the customer satisfaction survey and/or screen sharing, you can withdraw your consent at any time. If you choose to withdraw your consent, it does not affect the lawfulness of processing based on consent before its withdrawal. The withdrawal comes into effect from the time of withdrawal.

Misdirected emails received by NemLog-in Support are, to the extent that is possible, forwarded to the appropriate authority/unit.

### **9.1 Storage of your personal data for providing NemLog-in support**

The Danish Business Authority is our data processor for providing support on NemLog-in.

- With consent, the phone call is recorded and stored for 30 days, after which it is deleted. The call is recorded for training and quality assurance purposes.
- With consent to receive a customer satisfaction survey, your phone number is deleted after 90 days, and your comment is deleted after

180 days. The customer satisfaction survey is sent based on your call.

- If you choose to enter your civil registration number (CPR number) in the support phone menu, your civil registration number (CPR number) will be displayed to the supporter when your call comes through. Your civil registration number (CPR number) will not be saved and will disappear from the supporter's screen when the call is terminated.
- In the data processor's phone system, call data is deleted after 90 days (data includes phone number, date and time, call duration, queue selection, any callbacks, wait time, and supporter's name).
- For statistical purposes, data is stored in anonymised form for up to 5 years.
- With consent for screen sharing in the screen-sharing tool, the video session is stored for 90 days, after which it is automatically deleted. The session is recorded for training and quality assurance purposes.
- All written inquiries are stored for 6 months and then deleted.
- With consent to receive a customer satisfaction survey in relation to written inquiries, your email is deleted after 90 days, and your comment in the customer satisfaction survey is deleted after 180 days. The customer satisfaction survey is sent based on your written inquiry.
- All written inquiries that NemLog-in Support forwards to another authority are archived and stored. Any complaints will also be archived and stored.
- The data processor uses a data sub processor to analyse trends in user calls. This is done to improve the service of the support. The conversations are transferred to the sub-processor that immediately converts the speech to text and anonymises the text. The anonymised text is then used for trend analysis. The sub-processor stores the audio recording of the conversation for 30 days, after which it is deleted.

## **10. Personal data that is processed in the use of websites**

NemLog-in has the following websites:

- [nemlog-in.dk](https://nemlog-in.dk), including [tu.nemlog-in.dk](https://tu.nemlog-in.dk) and [broker.nemlog-in.dk](https://broker.nemlog-in.dk)

When you visit one of the above websites, cookies are used for statistical purposes to create an overview of the number of visitors and which parts of the website are visited. As a user, you have the option to click 'No thanks to cookies' if you do not wish to have your information collected.

[NemLog-in.dk: Cookies \(only in Danish\)](#)

[Tu.NemLog-in.dk: Cookies \(only in Danish\)](#)

[Broker.NemLog-in.dk: Cookies \(only in Danish\)](#)

## 11. Your rights

You have the following rights under the data protection regulation regarding our processing of data on you.

If you want to make use of your rights, you need to contact the Agency for Digital Government.

### **Right to access data (The right of access)**

You have the right to obtain the information we process about you, as well as additional information.

You can view the personal data that the Agency for Digital Government has registered about you at any time.

You can send a request to the Agency for Digital Government in one of the following ways:

- Via Digital Post to the Agency for Digital Government.
- Via postal mail to the Agency for Digital Government, Landgreven 4, 1301 Copenhagen K with the title "Processing of NemLog-in personal data".

### **Right to rectification (correction)**

You have the right to rectify inaccurate personal data on yourself.

If you use MitID Erhverv, we receive your personal data from the organisation you represent. Therefore, you need to contact a MitID Erhverv administrator in your organisation if you like to have inaccurate personal data on yourself corrected.

If you use your private MitID in NemLog-in services, you can read more about your right to rectification in MitID's privacy policy via the following link:

[MitID - Privacy notice](#)

**Right to erasure (Right to be forgotten)**

The Agency for Digital Government stores and processes your personal data for as long as it is necessary for the purpose of administration, management and operation of NemLog-in and NemLog-in's service areas.

In certain circumstances, you have the right to request the erasure of your personal data before our general erasure occurs. The rules concerning erasure are outlined in Article 17 of the General Data Protection Regulation (GDPR).

**Right to restriction of processing**

In certain cases, you have the right to restrict processing of your personal data.

However, restricting processing of your personal data may mean that you cannot use MitID or MitID Erhverv, and therefore cannot access the services in NemLog-in.

If you would like to request to restrict the processing your personal data, you should contact the Agency for Digital Government. See contact information above.

**Right to object**

In special situations, you have the right as a user to object to the processing of your personal data that the Agency for Digital Government has registered.

You can contact the Agency for Digital Government in one of the following ways:

- Via Digital Post to the Agency for Digital Government.
- Via letter to the Agency for Digital Government, Landgreven 4, 1301 Copenhagen K. with the title "Complaint about the processing of NemLog-in personal data".

**Right to transmit personal data (data portability)**

This right does not apply to NemLog-in, as data processing takes place as part of the exercise of official authority, which the data controller is required to by law.

**The right to withdraw consent**

The right to withdraw consent applies concerning support. When you request support, you may be asked to consent to the processing of your personal data for customer satisfaction analysis, screen sharing, and

call analysis. If you choose to withdraw your consent, it does not affect the lawfulness of the agency's processing of your personal information based on your previously given consent and up to the time of withdrawal. If you withdraw your consent, it only takes effect from the time withdrawal and henceforward.

Please note that there are exceptions to these rights, and you may not always be able to exercise all of your rights. This is because, as an official authority, we often process personal data as part of our exercise of official authority, and certain exceptions apply.

## **12. Complaint to the Danish Data Protection Agency**

You have the right to file a complaint with the Danish Data Protection Agency (Datatilsynet) if you are not satisfied with the way we process your personal data. You can find the contact information at the Danish Data Protection Agency's website.

[The Danish Data Protection Agency's website](#)

You can also contact the Agency for Digital Government directly if you would like to file a complaint about the way that the agency is processing your personal data.