



# Personal data protection policy

## Contents

<b>1. Purpose</b> .....	<b>3</b>
<b>2. Scope</b> .....	<b>3</b>
<b>3. Definitions</b> .....	<b>3</b>
3.1. Concept of personal data .....	3
3.2. Concept of sensitive data .....	3
3.3. Data subject .....	3
3.4. Personal data controller .....	3
3.5. Sub-contractor .....	3
3.6. Processing of personal data .....	4
3.7. Recipient .....	4
<b>4. Identity of the data controller and contact details</b> .....	<b>4</b>
<b>5. Personal data subject to processing</b> .....	<b>4</b>
5.1. Collection, purposes and legal basis .....	4
5.2. Consent .....	5
5.3. Retention period .....	5
5.4. Minimising the collection and retention of personal data .....	5
<b>6. Technical and organisational security measures</b> .....	<b>6</b>
<b>7. Data transfer to third countries</b> .....	<b>6</b>
<b>8. Data accuracy, accountability, transparency and rights of data subjects</b> .....	<b>7</b>
<b>9. Applicable law and jurisdiction</b> .....	<b>8</b>
<b>10. Monitoring and amendments to this policy</b> .....	<b>8</b>

## 1. Purpose

This document formalises the Denos Medical Assistance (DMA) personal data protection policy. It is a reference framework for data protection, detailing all the management and governance rules applicable to the protection of personal data within DMA.

## 2. Scope

This personal data protection policy applies to all DMA activities and is governed by the General Data Protection Regulation – GDPR. This policy applies to DMA and all its subsidiaries present in the territory of the European Union.

For subsidiaries outside the European Union, this policy applies if they process personal data relating to persons located in the territory of the European Union.

This personal data protection policy also applies to subsidiaries processing personal data located in countries outside the European Union to which the law of a Member State of the European Union applies.

For a DMA subsidiary or its new location outside the European Union, personal data processing of subjects who are not members of the European Union must be done in accordance with local regulations on personal data protection.

## 3. Definitions

### 3.1. Concept of personal data

This means any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier such as an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

### 3.2. Concept of sensitive data

This means personal data that directly or indirectly reveals the person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

### 3.3. Data subject

This means a natural person for whom personal data is collected or processed by DMA or by a DMA subcontractor, regardless of how it is used.

### 3.4. Personal data controller

The person responsible for processing personal data, meaning the natural or legal person who determines the purposes and methods of processing the data.

### 3.5. Sub-contractor

The sub-contractor is the natural or legal person, company or public body that processes personal data on behalf of the data controller, as part of a service or provision.

### 3.6. Processing of personal data

This concept means any operation involving personal data, regardless of the process used. For example, saving, organising, storing, modifying, transmitting personal data, or reconciling it with other data.

### 3.7. Recipient

The recipient means the person authorised, depending on their duties, to receive data saved in a file or processed.

## 4. Identity of the data controller and contact details

Data Controller: DENOS Medical Assistance, 42 avenue de la Grande Armée, 75017 Paris, Trade and Companies Registration No.: 525 151 890 Paris Trade and Companies Register Data Protection Officer: DPO@denosgroup.com.

## 5. Personal data subject to processing

DMA collects the information required to run its business and ensure smooth operation of the services offered.

This is essentially:

- Information relating to civil status (surname, first name, date of birth, place of birth, etc.)
- Contact details (telephone number, postal address, email address, etc.)
- Information relating to the person's occupation (employer, status, position, etc.)
- Health information necessary for the delivery of the DMA services subscribed (medical records, schedule of the care pathway, pathologies, etc.)

### 5.1. Collection, purposes and legal basis

Information collected	Purpose	Legal basis
<b>Information relating to civil status:</b> Surname, First name, date of birth, place of birth  <i>This data is given voluntarily</i>	<ul style="list-style-type: none"> <li>• Management of care pathways</li> <li>• Patient support</li> <li>• Monitoring of chronic diseases</li> <li>• Protection of the vital interests of the person concerned (e.g. medical emergency situation in life or death situation)</li> <li>• The processing of personal data is necessary to carry out a public interest mission</li> <li>• Management of DMA employees</li> </ul>	Our legitimate interest in providing an effective service, in accordance with our contractual obligations, in responding to any request or claim received.
<b>Contact details:</b> telephone number, postal address, email address		Our legitimate interest in exercising or defending the rights of the data subjects or our rights, in accordance with applicable legal provisions.
<b>Information relating to the person's occupation:</b> employer, status, position		Our legal, regulatory or ethical obligations (such as record keeping, fraud prevention).
<b>Health information:</b> information in medical records, planning and stages of care pathway, pathologies		<i>Consent of data subjects.</i> By deciding to provide us with
<b>Any other data that the data subjects decide to give us</b>		

Information collected	Purpose	Legal basis
		data that we have not requested, the data subjects agree that we may use it for the purposes mentioned.

## 5.2. Consent

The collection and processing of personal data requires the consent of the data subject, except in cases where the processing is the result of a legal obligation or contractual performance. Data subjects may revoke their consent at any time by contacting the data protection officer (see paragraph 9).

This consent may, depending on the DMA's terms of service (DMA services included in insurance cover, services offered independently of insurance policies, etc.) and depending on the nature of the personal data concerned:

- Be collected by the insurer or the insurance manager, DMA's partner;
- Be collected directly by DMA from the data subject.

In certain situations, the insurer or the insurance manager is required to collect consent so that the data it holds for its own purposes can be sent by its intermediary to DMA, to allow DMA to deliver the agreed services. If additional personal data is needed to perform DMA's services, DMA will directly collect the relevant consent from the data subject.

When collecting personal data, DMA ensures that the consent managed by insurers is transparent, by informing the data subjects how it uses their data and that it might be shared with third parties.

The data is collected fairly, and no collection is made without the person's knowledge.

## 5.3. Retention period

Personal data collected by DMA is retained for a limited period not exceeding the period required for the purposes of collection. For processing outside research activities, the retention period for health data is 10 years.

Special cases:

In certain specific situations, it is the responsibility of the data controller to carry out an assessment of the data retention period (e.g. in the event of death of a patient, relocation or redundancy, etc.).

## 5.4. Minimising the collection and retention of personal data

DMA collects, uses, transmits and processes the personal data that is required for the purposes identified in this personal data protection policy or permitted by law. If personal data is requested for purposes other than the purposes identified above, DMA will inform the data subjects of the new basis and new purpose and, if applicable, the respective consent for processing the personal data will be requested.

The personal data will be retained by DMA for the period required to perform the purpose for which it was collected and in accordance with legal requirements. In the event of a dispute, the data may be retained until expiry of the limitation period.

As personal data is collected on the basis of consent, it will be retained until the data subject expresses the right to object to further processing of their data, if no other basis prevails.

Data retention periods may be modified significantly when public interest archiving purposes, historical, scientific or statistical reasons are involved. In this case, DMA agrees to abide by the appropriate retention and safety measures.

The storage and retention of data for statistical purposes shall be proportionate to the purpose, respecting the essence of the right to protection of personal data and providing for adequate, specific measures to defend the fundamental rights and interests of the data subject.

When personal data is no longer needed, it will be irreversibly anonymised (in which case it is possible to retain and use anonymous information) or securely destroyed.

## 6. Technical and organisational security measures

DMA, in its capacity as data controller, endeavours to guarantee to the data subjects the security of the processing performed on the personal data and to avoid any breach of the GDPR (in particular: accidental or unlawful breach of security; destruction, loss, alteration of data, or unauthorised disclosure of personal data; unauthorised access to such data).

To this end, DMA puts in place appropriate technical and organisational measures, guaranteeing a level of security appropriate to the risks presented by the processing.

DMA has put in place technical and organisational security measures (physical, electronic and procedural) appropriate to the sensitivity of the information we store and process. In particular:

- We store and archive personal data in France
- We encrypt communication data and flows using state-of-the-art encryption algorithms
- We select digital technologies with the highest security standards
- We protect applications through strong authentication
- We differentiate the employee authorisation system according to the type of data concerned, the level of sensitivity and the employee's role
- We secure access to the premises
- We train and manage DMA employees in how to respect security and privacy when handling personal data
- In addition to the GDPR-related aspects, we confer "medical confidentiality" authorisation on all employees who need to access medical information in any form whatsoever, issuing a certificate that is renewed and updated every 2 years
- We have a charter for the secure use of IT resources by DMA employees

## 7. Data transfer to third countries

If the data processing carried out by DMA involves a transfer of personal data to a third country (located outside the European Union or not benefiting from an adequate level of protection within the meaning of European regulations) or to an international organisation, DMA undertakes to put in place measures guaranteeing the provisions of the GDPR regulations and ensure that its employees and subcontractors comply with them.

## 8. Data accuracy, accountability, transparency and rights of data subjects

DMA ensures that personal data is accurate, complete and up to date. Data owners should contact [dpo@denosgroup.com](mailto:dpo@denosgroup.com) by email to update their data when required.

All questions relating to DMA's privacy practices must be sent to the DMA Data Protection Officer at the following email address: [dpo@denosgroup.com](mailto:dpo@denosgroup.com) and/or postal address: DENOS Medical Assistance, for the attention of the Data Protection Officer (DPO), 42, Avenue de la Grande Armée 75017 Paris - France.

The data subject has the right, under the conditions and for the purposes of Articles 12 to 22 of the GDPR, to request from the data controller at any time:

- Provision of more details on how their personal data is used and processed
- Access to their personal data and the information provided for in the GDPR
- Rectification or erasure, without justified delay, including exercise of the right of limitation and the right "to be forgotten" where, in the absence of any other legal basis for the processing:
  - The personal data is no longer necessary for the purpose for which it was collected
  - The data subject withdraws their consent, only applicable in cases where this is the basis for the collection and processing of the data
  - The data subject objects to the processing of their data beyond the maximum retention period
- Restriction of data processing, if one of the following situations applies:
  - Challenge regarding the accuracy of personal data, after a sufficient period allowing the data controller to verify and update it
  - The processing is unlawful and the data subject objects to the deletion of the personal data and requests, in return, limitation of its use
  - The data controller no longer needs the personal data for processing purposes, but the data is required by the data subject for the purpose of declaring, exercising or defending a right in court
  - The data subject objects to the processing, until the legitimate basis has been verified by the data controller
- Data portability, so that the data subject can transmit the data to other controllers, if the processing is based on consent or if the processing is carried out by automated means
- Not be subject to automated individual decisions, including profiling
- The right to withdraw consent at any time, provided that consent is the basis on which the data is collected and processed, otherwise this compromises the lawfulness of the processing carried out on the basis of the consent previously given until the date of its withdrawal.

These rights, although recognised in the GDPR, are not absolute, so they need to be weighed in the light of DMA's legal obligations and therefore in the light of its rights and interests. Requests from data subjects will be processed within the limits set out in the GDPR.

For security and data protection reasons, when exercising one of the aforementioned rights, the data controller may require a document proving the identity of the data subject.

## 9. Applicable law and jurisdiction

This privacy and data protection policy is governed by French law.

In the event of a personal data breach constituting a risk to privacy (a loss of integrity, availability, and confidentiality), the CNIL will be notified as soon as possible, in accordance with Article 33 of the GDPR, at the latest within 72 hours. If the incident poses a high risk to the privacy of data subjects, the data subjects will also be notified.

## 10. Monitoring and amendments to this policy

This policy is a living document, which may be subject to change or replaced in a new version. The document must be systematically revised at least every 18 months, to include potential changes relating to DMA and the regulations. This revision is the responsibility of the DPO (Data Protection Officer).

Last updated May 2023