# PRACTITIONER - DOCTENA DATA PROCESSING AGREEMENT

**Version:** 2.0.0-20260201 **Effective Date:** February 1, 2026 **Language:** English **Publication URL:** https://cdn.doctena.com/legal/DPA/practitioners/2.0.0-20260201/DPA-practitioner-doctena-2.0.0-20260201-EN.pdf

---

## Legal Binding

This Data Processing Agreement is incorporated by reference into the contractual service agreement ("Principal Agreement") between the Controller and Doctena.

**No separate signature is required.** By signing the Principal Agreement, the Controller accepts the terms of this DPA in its entirety.

The applicable version of this DPA is specified in the Principal Agreement. This document is available at:

https://cdn.doctena.com/legal/DPA/practitioners/2.0.0-20260201/DPA-practitioner-doctena-2.0.0-20260201-EN.pdf

---

## Parties

This Data Processing Agreement (hereinafter referred to as the "Agreement" or "Addendum") forms part of the latest contractual service agreement (hereinafter referred to as the "Principal Agreement")

**between:**

The Practitioner or Practice, **as identified in the Principal Agreement** (hereinafter referred to as the "**Controller**")

**AND**

The Doctena entity **as specified in the Principal Agreement**, which shall be one of the following:

| **Country** | **Doctena Entity** | **Address** |
|---|---|---|
| Austria | Doctena Austria GmbH | Simmeringer Hauptstraße 24, 1110 Vienna |
| Belgium | Doctena Belgium Sprl | Square de Meeus 37, B-1000 Bruxelles |
| Belgium | Sanmax Sprl | Square de Meeus 37, B-1000 Bruxelles |
| Germany | Doctena Germany GmbH | Kurfürstendamm 14, 10719 Berlin |
| Luxembourg | Doctena SA | 42 Rue de la Vallée, L-2661 Luxembourg |
| Netherlands | Doctena Belgium Sprl | Square de Meeus 37, B-1000 Brüssel (Belgium) |
| Switzerland | Doctena Switzerland GmbH | Hagenholzstrasse 83b, 8050 Zürich |

(hereinafter referred to as the "**Processor**")

(hereinafter together referred to as the "**Parties**")

**Note:** The identity of both the Controller and the applicable Doctena entity (Processor) are specified in the Principal Agreement. This DPA applies to the parties as identified therein.

The terms used in this Agreement shall have the meanings set forth in this Agreement. Terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

The Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement.

---

## 1. Purpose

The purpose of the Agreement is to define the conditions to which the Processor undertakes to carry out, on the Controller's behalf, the personal data processing operations defined below.

As part of their contractual relations, the Parties shall undertake to comply with the applicable regulations on personal data processing and in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation which is applicable from 25 May 2018 (hereinafter referred to as the "GDPR").

Within the framework of the data controller's residence in Switzerland, the relevant local law must be complied with. This means that all legal matters related to taking up residence in Switzerland are to be handled in accordance with the laws and regulations of this country. This includes the Swiss Federal Act on Data Protection (DSG), which came into effect on September 1, 2023, along with its accompanying regulations. Data processing agreements between Doctena Switzerland GmbH and a controller with a corporate seat in Switzerland are subject to Swiss law,

and thus particularly to the Federal Act on Data Protection (DSG) along with its accompanying regulations.

---

## 2. Definitions

In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

**The terms "Process/Processing/Processed", "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data", "Processing Activities"**, and any other definition not included in this agreement or the main contract have the same meaning as in the GDPR or the Swiss DPA (Data Protection Act). Thus, the mentioned terms are understood not only in the context of the EU's GDPR but also according to the provisions of the Swiss DPA. The applicable law is the one resulting from point 1.

**"EU"** means European Union.

**"EEA"** means the European Economic Area.

**"Third country"** means any country outside EU/EEA, except where that country is the subject of a valid adequacy decision by the European Commission on the protection of Personal Data in Third Countries.

**"Services"** means the services to be supplied by the Processor to the Controller pursuant to the Principal Agreement.

---

## 3. Duration of the Agreement

This Agreement enters into force on digital signature of this document or when signed and explicit mention of the date on last page (hereinafter referred to as the "Agreement Effective Date") and until the end of the Principal Agreement.

The Controller has commissioned the Processor to provide Services until the end of the Principal Agreement.

---

## 4. Controller's Obligations

The Controller has primary responsibility and undertakes to:

1. provide the Processor with clear and sufficiently documented instructions if he/she requested specific requirements not included in Principal Agreement regarding the agreed Services;

2. document, in writing, any instruction bearing on the processing of data by the Processor;

3. provide the Processor with the data mentioned under point 5 of the Agreement;

4. keep a register of the Processing activities under his/her own responsibility;

5. implement from his/her side all technical and organisational security measures to ensure a sufficient level of protection for Personal Data processed using the Processor's Services;

6. To ensure compliance with the obligations set forth in the GDPR before and during processing; to the extent that residence in Switzerland is established, the data controller commits to ensuring compliance with the obligations defined in the DPA before and during processing, as far as his area of responsibility is concerned; the data processor,

in turn, ensures compliance with the obligations recorded in the DPA within his area of responsibility as well;

7. respect the rights of the Data Subject;

8. notify any security incidents to the processor regarding the provided Services;

9. supervise the processing, including by conducting audits and inspections with the Processor when deemed necessary;

10. when using the AI Telesecretary feature, comply with the additional obligations set forth in Section 5a.6.

---

## 5. Description of the Processing Being Subcontracted

The Controller has commissioned the Processor to provide, on his behalf, for the following services:

(i) Management of patient's data regarding his/her practitioner's appointment and follow-up services;

(ii) Management of the practitioner's agenda/calendar;

(iii) Management of the IT infrastructure, software, maintenance and administration related to the Principal Agreement services.

The nature of operations carried out on the data for the purpose of (i), (ii) and (iii) are:

- Collection, storage and modification of personal information of patient required by the practitioner to organize the appointment
- Search of patient account using one of its stored personal data

- Communications with data subject regarding appointment using email or (mobile) number
- Data imports into Doctena services using Practitioner provided structured data (e.g. Onboarding)
- Automated backup of data

The Processor shall undertake to process the data solely for the purpose(s) subject to the Principal Agreement and above mentioned purposes.

The category of data subjects is: **Patients**.

In order to provide the services mentioned under (i), (ii) and (iii), the Processor is authorised to process, on behalf of the Controller, the following necessary personal data information categories, depending on the data provided by the Controller and/or the Data Subject:

1. **Personal data of identification**: name, title, email, address (private and professional), previous addresses, (mobile) phone number (private, professional), identifiers attributed by the Controller;

2. **Personal details**: age, sex, date of birth, place of birth, registry office and nationality;

3. **Data of electronic identification**: IP addresses, cookies, moments of connection, electronic signature;

4. **Data relative to the care**: data relative to resources and procedures used for the medical and paramedical care of the patients (e.g. practitioner/patient notes, reason of visit);

5. **Details of the other members of the family or the household**: children, supported people, other members of the household, information on parents and relatives;

6. **Pseudonymisation**: Controls to protect Confidentiality, Integrity and Availability of data (e.g. hashed credentials);

7. **(only if option is activated) Data of identification**: emitted by public services, e.g. national identification number, social security number, number of ID card, passport.

---

## 5a. AI Telesecretary Processing (Optional Feature)

This section applies only when the Controller has activated the AI Telesecretary feature through the Doctena platform. The processing described in this section is in addition to the processing described in Section 5.

### 5a.1 Scope and Activation

The AI Telesecretary is an optional feature that enables automated telephone call handling for appointment scheduling. This feature is activated at the Controller's discretion through the Doctena platform settings.

### 5a.2 Additional Processing Activities

When the AI Telesecretary feature is activated, the Controller commissions the Processor to provide, on his behalf, the following additional services:

(iv) AI-powered telephone call handling for appointment scheduling;

(v) Voice recording and transcription of telephone calls;

(vi) Automated call routing and natural language processing.

The nature of operations carried out on the data for the purpose of (iv), (v) and (vi) are:

- Reception and handling of incoming telephone calls via AI voice assistant
- Recording of telephone conversations (with prior disclosure to caller)

- Automated speech-to-text transcription of call recordings
- Natural language processing for intent recognition and appointment booking
- Automated routing decisions for multi-practitioner practices
- Storage and retrieval of call recordings and transcripts for quality assurance

### 5a.3 Additional Data Categories

In addition to the data categories listed in Section 5, the following personal data categories are processed when the AI Telesecretary feature is activated:

8. **Voice data**: Audio recordings of telephone calls, voice characteristics;

9. **Transcripts**: Text transcriptions of recorded calls generated through automated speech-to-text processing;

10. **Call metadata**: Call duration, timestamps, routing decisions, AI confidence scores, language detected.

Voice data and transcripts may contain Special Categories of Personal Data (health data) as defined in Article 9 of the GDPR when patients describe symptoms or reasons for their appointment during the call.

### 5a.4 AI Transparency and Disclosure

In accordance with Article 50 of Regulation (EU) 2024/1689 (EU AI Act) and the transparency requirements of the GDPR:

a) The AI Telesecretary is classified as a High-Risk AI system under Annex III, point 5 of the EU AI Act (AI systems intended for use in healthcare);

b) Every call handled by the AI Telesecretary begins with a mandatory vocal disclaimer informing the caller that:

- They are speaking with an AI-powered assistant;

- The call may be recorded;
- They may end the call at any time;

c) The Processor (Doctena) configures the mandatory vocal disclaimer during onboarding. It is the sole responsibility of the Controller to ensure that this GDPR-compliant disclaimer remains active and unmodified;

d) The Controller acknowledges their obligation under Art. 26 of the EU AI Act regarding deployment of high-risk AI systems.

### 5a.5 Controller Obligations for AI Features

When using the AI Telesecretary feature, the Controller additionally undertakes to:

1. Not modify or disable the mandatory vocal disclaimer configured by Doctena during onboarding;
2. Ensure patients are informed about AI processing in the practice's privacy notice;
3. Provide a human fallback option during practice opening hours;
4. Review AI-generated bookings regularly and correct errors promptly;
5. Report any AI system malfunctions to the Processor without undue delay;
6. Maintain the ability to disable the AI Telesecretary feature if required;
7. Ensure staff are trained on the AI Telesecretary's capabilities and limitations.

### 5a.6 Human Oversight and Fallback

In accordance with EU AI Act requirements for human oversight of high-risk AI systems:

a) The Controller maintains access to all call recordings and transcripts via the Processor's platform for review and quality assurance;

b) Appointments booked by the AI Telesecretary appear in the Controller's calendar system and may be modified or cancelled by the Controller;

c) The Controller retains full control over the AI Telesecretary's configuration, including operating hours, language settings, and knowledge base content.

---

## 6. Processor's Obligations

As long as the Processor processes Personal Data for the Controller, the following conditions apply in accordance with Article 28 of the GDPR:

### Obligations of the Processor towards the Controller

1. The Processor undertakes to comply with all statutory provisions of the GDPR and national law regarding data protection and to operate data processing (logical and physical) exclusively within the EU or the EEA. Any form of relocation of the data processing (including the transfer of the place of business of the Processor) to a third country (outside the EU or the EEA) requires the express prior written consent of the Controller.

2. The Processor shall undertake to process the data in accordance with the documented instructions from the Controller. Where the Processor is obliged to transfer personal data to third country or an international organization, under EU Law or Member State law to which the Processor is subject, the Processor shall inform the Controller of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3. If the Processor considers that a directive issued by the Controller violates the GDPR or other data protection laws of the EU or a Member State, the Processor must inform the Controller without delay and in bona fide.

4. The Controller is entitled to check compliance with all applicable data protection regulations and compliance with the contractual provisions themselves or through third parties with the Processor and any subcontractors. For this purpose, the Processor provides the Controller with the necessary documentation for allowing the Controller, or any other third party it has authorized, to conduct audits, including inspections, and contributes to such audits.

5. The Processor shall provide the Controller with all the necessary information to demonstrate compliance with its obligations imposed in the Agreement.

6. The Processor shall undertake to process the data solely for the purpose(s) subject to the Principal Agreement.

**Records of Processing Activities**

7. The Processor shall implement the data processing in a documented manner, unless he is required to do differently by the law of the EU or of the Member States to which the Processor is subject; in such a case, the Processor shall inform the Controller of these legal requirements prior to processing, unless the law in question prohibits such communication because of a significant public interest.

8. According to Article 30 of the GDPR, the Processor maintains a written record of all categories of processing activities carried out on behalf of the Controller, containing:

    - the name and contact details of the Controller on behalf of which the Processor is acting, any other processors and, where applicable, the data protection officer;
    - the categories of processing carried out on behalf of the Controller;
    - where applicable, transfers of personal data to third country or an international organization, including the identification of that third country or international

organization and, in the case of transfers referred to in the second subparagraph of Article 49 (1) of the GDPR, the documentation of suitable safeguard;

- where possible, a general description of the technical and organizational security measure, including inter alia:
    - The pseudonymisation and encryption of personal data;
    - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

To the extent that residence in Switzerland is established, the data processor, in accordance with Art. 12, paragraph 3 of the DPA, maintains a record of all types of processing activities carried out on behalf of the data controller, containing the following information:

- The identity of the controller and the processor;
- The purpose of the processing;
- A description of the categories of data subjects and the categories of personal data processed;
- The categories of recipients;
- If possible, the period for which the personal data will be stored, or the criteria used to determine that period;
- If possible, a general description of the security measures to ensure data protection according to Article 8 DPA;
- If the data is disclosed abroad, the indication of the country as well as the guarantees according to Article 16, paragraph 2 DPA.

**Technical and Organisational Measures**

9. The Processor shall undertake to take into consideration, in terms of its tools, products, applications or services, the principles of data protection by design and by default.

10. The Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 of the GDPR (taking technical and organizational measures, security breach notification, compilation of a privacy impact assessment). The Processor assists the Controller in carrying out privacy impact assessment on Data Protection. The Processor assists the Controller with regard to prior consultation of the competent supervisory authority.

11. The data processor implements appropriate technical and organizational measures to ensure a level of security for the data and/or data processing that is appropriate to the identified risks. This obligation follows from Article 32 of the GDPR and, to the extent of residence in Switzerland, from Article 8 of the DPA in conjunction with Article 3 of the DPO (Data Protection Ordinance). This includes implementing the provisions of the Federal Council on the minimum requirements for data security according to the Data Protection Ordinance (DPO). These include, among others:

    - the pseudonymisation and encryption of personal data;
    - the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The security measures are intended to protect Personal Data from destruction or accidental or unlawful loss, alteration, unauthorized disclosure or access.

**Data Protection Officer**

12. The data processor informs the data controller of the name and contact details of its data protection officer, if one has been appointed in accordance with Article 37 of the GDPR. To the extent that residence in Switzerland is established and a data protection advisor

has been appointed, the controller publishes the contact details of the data protection advisor in accordance with Article 10, paragraph 3, lit. d) of the DPA and communicates these to the EDÖB.

https://cdn.doctena.com/legal/dpo.html

## Sub-contracting

13. Subcontracting or the use of subcontractors (hereinafter "Subcontractors") is fundamentally permitted for the data processor. Data transfer is only allowed within the scope defined by section 6, subsection 1 of this contract. The data controller is informed in advance about the intended subcontracting or the intended use of Subcontractors, and the data controller is free to object to this subcontracting within 14 days. The data processor must oblige all Subcontractors, in the sense of Article 28, paragraph 4 of the GDPR, to fulfill their contractual obligations and transfer all obligations that the data processor must fulfill to the Subcontractor. The data processor only works with Subcontractors who provide sufficient guarantees that appropriate technical and organizational measures are taken to ensure that processing is carried out in accordance with these regulations and that the rights of the data subject are protected. Subcontractors are prohibited from processing or transmitting data in a third country.

To the extent of residence in Switzerland, this follows from Art. 9, para. 3 of the DPA and applies equally, as described under point 13.

A list of Subcontractors can be found on the website below:

https://cdn.doctena.com/legal/sub-processors.html

## Confidentiality and Security

14. The Processor shall ensure that authorised persons who process or have or can obtain access to the data processed, have committed themselves to confidentiality prior to processing or accessing to such data, unless they are nevertheless subject to an

obligation of confidentiality, as well as ensuring the appropriate data protection awareness and training.

15. The Processor shall undertake all reasonable steps to protect the personal data processed hereunder. A list of our security measures can be found on the website below:

https://cdn.doctena.com/legal/security.html

### Data Subject's Rights to Information

16. At the time data are collected, the Processor must provide the Data Subjects concerned by the processing operations with information about the data processing it carries out.

### Exercise of Data Subject's Rights

17. If a Data Subject contacts the Data Processor or a Subcontractor instead of the Data Controller, and it falls outside the responsibility of the Data Processor, the Data Processor informs the Data Subject that their request must be directed to the Data Controller directly. The Data Processor will not forward these requests to the Data Controller.

18. The Processor shall assist the Controller, insofar as possible, with appropriate technical and organisational measures for the fulfilment of its obligation to respond to requests of Data Subject exercising their rights referred to in Chapter III of the GDPR (inquiry, right of access, to rectification and erasure, information, data portability, opposition, and automated decision-making in individual case including profiling) within a reasonable time.

### Notification of Personal Data Breaches

19. The Data Processor informs the Data Controller about any data breaches without undue delay and no later than 48 hours after becoming aware of it, via email, in accordance with Article 33(2) of the GDPR. This notification must be accompanied by all necessary documentation so that the Data Controller can report this breach to the relevant supervisory authority if necessary.

To the extent that the Controller is based in Switzerland, Article 24(3) of the DPA applies. Accordingly, the Processor must report any data security breach to the Controller as quickly as possible.

**Fate of the Personal Data**

20. The Data Processor will, at the choice of the Data Controller or upon termination of the main contract, permanently delete or return all data unless there is an obligation under EU or national law to retain the personal data. It is the responsibility of the Data Controller to inform the Data Processor in writing upon termination of the main contract about whether and how a data export should take place. Data from database backups will only be permanently removed after a complete backup cycle of 3 months.

21. The Controller is given the option to configure the data retention period. By default all data is kept for 10 years which can be reduced up to 1 year according to the Controller's needs.

---

## 7. Additional Agreements

1. In accordance with Article 83 of the GDPR / Art. 60 et seq. of the DPA, a fine may be imposed on the Data Controller or Processor who fails to comply with certain data protection obligations, especially those arising from the GDPR/DPA requirements. The applicable law is decisive.

---

## Version History

| Version | Date | Summary of Changes |
|---|---|---|
| 1.0.0-20240209 | 2024-02-09 | Initial version |

| Version | Date | Summary of Changes |
|---|---|---|
| 2.0.0-20260201 | 2026-02-01 | Added Section 5a (AI Telesecretary Processing); Added item 10 to Section 4 (Controller Obligations) |

---

## Publication

This document is published at:

https://cdn.doctena.com/legal/DPA/practitioners/2.0.0-20260201/DPA-practitioner-doctena-2.0.0-20260201-EN.pdf

For questions regarding this DPA, please contact Doctena's Data Protection Officer:

https://cdn.doctena.com/legal/dpo.html