

LEGAL

Data processing agreement

LAST UPDATED · 14 OCT 2026

Radiant Science UG (haftungsbeschränkt)

Floningweg 16, 12107 Berlin, Germany

Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Agreement, as defined in the Radiant Science Terms of Service available at www.radiantscience.io/terms (the "Terms"), between the Customer and Radiant Science UG (haftungsbeschränkt) ("the Company"). The Customer accepts this DPA when it accepts the Terms, and in any event before the Company processes Personal Data on its behalf. Where the Services are provided through a Reseller, each End Customer accepts this DPA directly with the Company before activation, and references to the Customer apply to that End Customer.

Whereas

- (A) The Customer acts as a 'Data Controller'. The Company acts as a 'Data Processor'.
- (B) The Customer wishes to subcontract Company Services, which may imply the 'Processing' of 'Personal Data' by the Company.
- (C) The Parties seek to implement a DPA that complies with the requirements of the current legal framework in relation to data processing, including Article 28 of the UK GDPR and, where applicable, Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).
- (D) Annex I, II and III are integral to this DPA and provide details about the Processing activities.

1. Definitions

1. "Agreement": has the meaning given in the Terms, and includes this DPA and its Annexes.

2. “Anonymised Data”: means data derived from Customer Personal Data by the anonymisation described in Section 9, which no longer relates to an identified or identifiable natural person.
3. “Call Content”: means all Customer Personal Data created because of a call handled by the Services, including the call recording, the transcript, the call record and summary, details collected during the call, messages and forms sent or received because of the call, and internal session data and quality-monitoring data relating to the call.
4. “Cessation Date”: means the date on which the Agreement, or the relevant End Customer's Subscription, ends.
5. “Company” / “Processor”: shall mean the entity providing the Services to the Customer, namely Radiant Science UG (haftungsbeschränkt).
6. “Confidential Information” / “Proprietary Information”: means all information (in any form) that concerns a Party's business operations and which any reasonable person would consider to be confidential. This would include, but not be limited to: trade secrets, methods, strategies, client lists, pricing, and other business processes and Customer Personal Data.
7. “Customer Personal Data”: means any Personal Data, including sensitive Personal Data Processed by the Company on behalf of the Customer in delivering the Services outlined in the Agreement.
8. “Data Controller” / “Controller”: shall mean the Customer that makes Customer Personal Data available to the Company.
9. “Data Protection Legislation”: has the meaning given in the Terms.
10. “EEA”: means the European Economic Area.
11. “Services”: means Company Services provided under the Agreement and this DPA.
12. “Sub-Processor”: means any person appointed by or on behalf of the Company to process Personal Data on behalf of the Customer in connection with the Agreement.

Capitalised terms not defined in this DPA (including "Applicable Law", "Customer Data", "End Customer", "Reseller", "Subscription" and "Third-Party Applications") have the meaning given in the Terms. The terms “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the UK GDPR, and their cognate terms shall be construed accordingly.

2. Company Obligations

1. The Company shall, in delivering the Services: (a) comply with Data Protection Legislation in the Processing of Customer Personal Data; (b) not Process Customer Personal Data other than as required to provide the Services or on the Customer's documented instructions; the Customer's documented instructions include the retention, deletion and anonymisation described in this DPA; and (c) not sell Customer Personal Data, use it for advertising, or disclose it to third parties for their own purposes.

2. If Applicable Law requires the Company to Process Customer Personal Data other than on the Customer's instructions, the Company shall inform the Customer of that legal requirement before Processing, unless that law prohibits it.
3. In the event the Company reasonably believes that an instruction issued by the Customer would violate Data Protection Legislation, the Company shall promptly notify the Customer.
4. If the Company cannot comply with the terms of this DPA for whatever reason, then the Company shall promptly inform the Customer of the inability to comply.
5. The Company hereby undertakes that, upon the Customer's request, the Company will cooperate with the Customer to enable the Customer to: (a) comply with reasonable requests of access, rectification, and/or deletion of Personal Data arising from a Data Subject; (b) enforce rights of Data Subjects under Data Protection Legislation; and/or (c) comply with all requests from a Supervisory Authority, including but not limited to in the event of an investigation.

3. Customer Obligations

1. The Customer shall ensure that its instructions, its use of the Services and the Customer Personal Data it makes subject to the Services comply with Data Protection Legislation and do not cause the Company or the Customer to breach any laws, rules or regulations. The Customer assumes full liability for collecting and processing Customer Personal Data in compliance with Data Protection Legislation.
2. The Customer is solely responsible for:
 1. the accuracy, quality and legality of Customer Data, including sensitive Customer Personal Data, and the means by which the Customer acquired such data;
 2. having a lawful basis under Data Protection Legislation for all Data Subjects whose Personal Data is processed by the Company as part of the Services, and for meeting all transparency requirements, including any notices to Callers and Patients and any necessary consents and authorisations;
 3. having the right to transfer, or provide access to, the Customer Personal Data to the Company for Processing in accordance with the Agreement; and
 4. configuring the Services appropriately for the Customer Personal Data, including the retention period, the access of its Authorised Users and the Third-Party Applications it connects.
3. The Customer will inform the Company without undue delay if it is not able to comply with its responsibilities under this Section or Data Protection Legislation, and will promptly notify the Company where it becomes aware that any Personal Data processed as part of the Services is inaccurate, out-of-date or incomplete, providing correct, up-to-date and full Personal Data in that event.
4. The Customer instructs the Company to process Customer Personal Data in accordance with this DPA. The subject matter, duration, nature and purpose of the Processing, the categories of Data Subjects and the types of Personal Data processed are set out in Annex I, II and III.

4. Resellers and Single Sign-On

- 1 . Where the Services are provided through a Reseller, the End Customer is the Controller of the Patient Data and other Personal Data in its Customer Data, and the Company processes that data as its Processor under this DPA.
- 2 . Where a Reseller supplies the Company with Personal Data of its own users and of End Customer staff, for example through a single sign-on, the Reseller is the Controller and the Company the Processor of that data, and this DPA applies to that data with the Reseller as the Customer.

5. Personnel

The Company shall take reasonable steps to ensure the reliability of its employees, agents and contractors, and of those of its Sub-Processors, who may have access to Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Security

- 1 . Taking into account industry best practices, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall in relation to the Customer Personal Data implement appropriate technical and organisational measures (Annex III) to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR. The Company may update these measures from time to time, provided that such updates do not materially reduce the overall security of the Services.
- 2 . In assessing the appropriate level of security the Company shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
- 3 . The Parties agree that the measures set out in Annex III provide an appropriate level of security for the Customer Personal Data, accounting for the risks presented by the processing outlined in the Agreement.

4. The Company maintains the following security certifications and compliance programmes, which are reviewed and renewed on an annual basis: a. Cyber Essentials: the Company holds a current Cyber Essentials certificate issued under the UK Government's National Cyber Security Centre (NCSC); b. NHS Data Security and Protection Toolkit (DSPT): the Company completes the NHS DSPT assessment annually and maintains a current submission demonstrating compliance with the National Data Guardian's data security standards applicable to organisations handling NHS patient data; c. ICO Registration: the Company is registered with the Information Commissioner's Office as a Data Controller and Data Processor under the UK GDPR and Data Protection Act 2018 (ICO Registration Number: ZB842255).
5. The Company shall implement and maintain the Technical and Organisational Measures set out at www.radiantscience.io/tom, which include as a minimum: a. access controls limiting Customer Personal Data to authorised personnel only, on a need-to-know basis; b. encryption of Customer Personal Data in transit and at rest; c. regular security assessments and vulnerability management processes; d. staff training and contractual obligations on sensitive health data protection and information security obligations; e. incident detection and response procedures, including the breach notification obligations set out in this DPA.

7. No Model Training

1. The Company shall not use Customer Personal Data, including call audio, transcripts, summaries or Patient Data, to train, fine-tune or otherwise improve any artificial-intelligence model operated by the Company or by any third party.
2. The Company shall contractually prohibit its Sub-Processors from using Customer Personal Data to train, fine-tune or otherwise improve their models, and shall configure each Sub-Processor to the shortest data retention it offers for the Services used.

8. Retention During the Services

1. Call Content is retained for the duration of the Agreement and is deleted or anonymised in accordance with Section 14 after the Cessation Date.
2. The Customer may instead instruct a shorter retention period of 30, 90, 180 or 365 days after the end of each call, by setting it in the Services or by written instruction to the Company. The same period applies to all Call Content of a call.
3. At the end of the applicable retention period the call recording is deleted, the transcript and call record are anonymised as described in Section 9, and the identifiable originals are deleted. Call Content cannot be retrieved after that point.
4. Patient records and caller phone numbers held to recognise returning callers are retained for the duration of the Agreement, unless deleted earlier on the Customer's instruction or under Section 11.

5. The Customer may request the deletion of an individual call through the Services or in writing. The call is withheld from the Customer's users once the request is made, and the Company permanently deletes its Call Content within thirty (30) days of the request.
6. The Company keeps records of access to Customer Personal Data and of significant system events. These records do not contain Call Content, and any message content they hold is removed at the end of the call's retention period.

9. Anonymisation

1. The Customer instructs the Company to anonymise the transcript and call record of each call at the end of its retention period, and before deletion after the Cessation Date, so that they can no longer be linked to an identified or identifiable natural person.
2. Anonymised Data is not Customer Personal Data. It is used only to maintain and evaluate the quality of the Services and is never used to train, fine-tune or otherwise improve any artificial-intelligence model. The Company shall not attempt to re-identify Anonymised Data and shall not disclose it in a form that identifies the Customer, any End Customer, any Patient or any Caller.
3. Where anonymisation of a call cannot be completed, the Company retries it and otherwise deletes the call without keeping a copy.

10. Sub-Processing

1. The Customer hereby provides the Company with general written authorisation to engage Sub-Processors to access and process Personal Data. At the time of accepting the Agreement, the Sub-Processors listed in Annex II are deemed to be approved.
2. The Company will impose contractual obligations on its Sub-Processors, and contractually obligate its Sub-Processors to impose contractual obligations on any further Sub-Processors which they engage to process Personal Data, which provide the same level of data protection for Personal Data in all material respects as the contractual obligations imposed in this DPA, including Section 7. The Company remains liable to the Customer for the performance of its Sub-Processors' obligations.
3. The Company will notify the Customer at least 14 (fourteen) days in advance (by email and by notice in the Service) of any changes to the list of Sub-Processors (Annex II).
4. The Customer may reasonably object to the Company's use of a new Sub-Processor (e.g., if making Personal Data available to the Sub-Processor may violate Data Protection Legislation or weaken the protections for such Personal Data) by notifying the Company promptly in writing within fourteen (14) business days after receipt of the Company's notice.

5. Such notice shall explain the reasonable grounds for the objection. In the event the Customer objects to a new Sub-Processor, as permitted in the preceding paragraph, the Company will use commercially reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening the Customer. If the Company is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Order Form(s) with respect only to those Services that cannot be provided by the Company without the use of the objected-to new Sub-Processor by providing written notice to the other party. The Company will not refund the Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services.

11. Data Subject Rights

1. Taking into account the nature of the Processing, the Company shall assist the Customer by implementing appropriate technical and organisational measures, for the fulfilment of the Customer obligations, as reasonably understood by the Company, to respond to requests to exercise Data Subject rights under Data Protection Legislation.
2. The Company shall: (a) promptly notify the Customer if it receives a request from a Data Subject under Data Protection Legislation in respect of Customer Personal Data; (b) ensure that it does not respond to that request except on the documented instructions of the Customer or as required by Applicable Law to which the Company is subject, in which case the Company shall to the extent permitted by Applicable Law inform the Customer of that legal requirement before the Company responds to the request.
3. Where a Data Subject's erasure request reaches the Company, the Company forwards it to the Customer, who may object within seven (7) days, for example because it must retain the data by law. Unless the Customer objects, and in any case where the Customer instructs erasure, the Company completes the erasure within fourteen (14) days of receiving the request or instruction.
4. Anonymised Data is outside the scope of access, rectification and erasure requests, because it can no longer be linked to the Data Subject.

12. Personal Data Breach

1. In the event of a Personal Data Breach arising during the provision of the Services by the Company, the Company shall:
 1. Notify the Customer about the Personal Data Breach without undue delay, but no later than forty-eight (48) hours, after becoming aware of the Personal Data Breach;
 2. Provide, to the extent reasonably available at the time of notice, a description of the nature of the breach, the categories and approximate number of Data Subjects affected, the categories and approximate number of data records affected, the likely consequences of the Breach, the risks to affected Data Subjects, the measures taken or proposed to address the breach and mitigate its possible adverse effects, and the name and contact details of the Company's contact point for the breach; promptly update the Customer as additional relevant information becomes available;
 3. Take all actions as may be required by Data Protection Legislation;
 4. Maintain records of all information relating to the Breach, including the results of its own investigations and authorities' investigations as well as remedial actions taken, for six (6) years after the incident is closed.
2. The Customer, as Controller, is responsible for notifying the competent Supervisory Authority and affected Data Subjects where required. The Company shall assist the Customer with the information reasonably required for those notifications.
3. Unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as blocked log-in attempts, pings, port scans and other network attacks that do not result in access to Customer Personal Data, are not Personal Data Breaches. Notification of a Personal Data Breach is not an acknowledgement of fault or liability by the Company.

13. Data Protection Impact Assessment and Prior Consultation

The Company shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required by Article 35 or 36 of the UK GDPR or equivalent provisions of Data Protection Legislation, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Company and its Sub-Processors.

14. Deletion or Return of Customer Personal Data

1. Export. On request made when the Agreement ends, and in any case within the period set out in Section 14.6 of the Terms, the Company provides an export of the Customer Personal Data still retained under this DPA, in a commonly used format. The export is prepared at the Cessation Date and remains available until the deletion under Section 14.2.

2. Deletion. Within thirty (30) days of the Cessation Date, the Company shall delete and/or procure the deletion of all copies of Customer Personal Data, unless the Parties agree otherwise in writing or Data Protection Legislation or other applicable legal or regulatory requirements require storage of the Customer Personal Data for a longer period. Where Customer Personal Data is retained under this exception, this DPA continues to apply to it until it is deleted. Call Content is anonymised before deletion as described in Section 9; Anonymised Data is not subject to this deletion.
3. Backups. Customer Personal Data held in rolling database backups, or in storage-level recovery copies of recordings, is not used or restored and ages out within seven (7) further days.
4. Confirmation. The Company confirms the deletion to the Customer in writing within fifty-two (52) days of the Cessation Date.

15. Audit Rights

1. Subject to this Section, the Company shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of Customer Personal Data by the Company and, through the information the Company obtains from them, its Sub-Processors. Information and audit rights of the Customer only arise under this Section to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Legislation.
2. The Customer shall give the Company reasonable prior written notice, not fewer than fourteen (14) business days in advance, of any audit or inspection to be conducted under this Section and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing any damage, injury, or disruption to the Company.
3. The Customer and the Company shall mutually agree upon the scope, timing, and duration of the audit or inspection. The Customer will pay any reasonably incurred costs and expenses incurred by the Company in the event the Customer performs an audit that is not (a) required by Data Protection Legislation, or (b) in response to a Personal Data Breach.
4. The scope of the audit rights is limited to reviewing the Company's relevant documentation, systems, and procedures directly related to the processing of the Customer's Personal Data, including security measures, data protection practices, and compliance records. The scope of audit rights does not extend to physical premises where the Personal Data is processed.
5. An audit may not be requested more than once in a 12 months period, unless there are indications of non-compliance and/or it is required by a Supervisory Authority or other regulatory authority responsible for the enforcement of Data Protection Legislation.

16. Processing Locations and Data Transfers

1. The Company hosts the Services, their databases, storage and backups in the United Kingdom (Microsoft Azure UK South). Sub-Processors that process Call Content do so in the United Kingdom or the European Union, as stated for each in Annex II.
2. The Parties rely on the adequacy decision for the transfer of Personal Data from the UK to the EEA under Article 45 of the UK GDPR to transfer Personal Data to the Company.
3. The Customer provides the Company with general written authorisation to transfer Personal Data outside of the EEA and the UK or to a jurisdiction which does not have adequacy status provided that the Company complies with the EU and the UK GDPR's international transfer rules and relies on an appropriate mechanism under Article 46 of the EU and the UK GDPR, namely the EU Standard Contractual Clauses and, for restricted transfers from the United Kingdom, the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment.
4. If a transfer mechanism relied on under this Section is invalidated or ceases to apply, the Parties shall cooperate in good faith to put in place an appropriate alternative mechanism recognised under Data Protection Legislation.

17. Government and Third-Party Requests

1. If the Company receives a legally binding request from a public authority or other third party for access to Customer Personal Data, it shall, unless the law prohibits it, promptly notify the Customer and refer the requester to the Customer.
2. The Company shall assess the lawfulness of the request, challenge it where it has reasonable grounds to consider it unlawful, and disclose only the minimum Customer Personal Data required to comply with it.
3. The Company does not give any public authority direct access to its systems or to Customer Personal Data.

18. Term, Precedence and Changes

1. This DPA takes effect on the date the Customer first accepts the Agreement or accesses the Services, whichever is earlier. It continues to apply after the Agreement ends until the Company has stopped all Processing of Customer Personal Data and completed Section 14.
2. Where the EU Standard Contractual Clauses, the International Data Transfer Agreement or the UK Addendum apply, they prevail over this DPA and the rest of the Agreement. Otherwise, the order of precedence in Section 1.4 of the Terms applies, under which this DPA prevails over the Terms with respect to the Processing of Customer Personal Data.

3. The Company may update this DPA in accordance with the section of the Terms on changes to the Terms. Material changes are communicated to the Customer at least fourteen (14) days before taking effect.

19. Confidentiality and Notices

1. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Proprietary Information”) confidential and must not use or disclose that Proprietary Information without the prior written consent of the other Party except to the extent that: (a) Disclosure is required by law; (b) The relevant information is already in the public domain.
2. All notices and communications given under this DPA must be in writing. Valid methods of notice include: notification via the Company dashboard and email. Dashboard notifications and emails to the Customer's registered account email address constitute valid written notice for the purposes of this DPA. Notices to Radiant Science UG should be sent to info@radiantscience.io or via the dashboard. Notices to the Customer will be sent to the email address registered at onboarding.

20. Governing Law and Jurisdiction

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation will be governed and construed in accordance with the laws of England and Wales. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

21. Liability

The liability of each party under this DPA is subject to the exclusions and limitations of liability and the indemnities set out in the Terms.

Annex I

List of Parties

Data Controller ("The Customer")

Name: As provided by Customer during account registration on the Radiant Science platform or in the Order Form.

Address: As provided by Customer during account registration on the Radiant Science platform or in the Order Form.

Contact person's name, position, and contact details: As provided by Customer during account registration on the Radiant Science platform or in the Order Form.

Activities relevant to the data transferred under these Clauses: Processing the Personal Data in order to provide the Company Services as detailed in the Agreement.

Data Processor ("The Company")

Name: Radiant Science UG (haftungsbeschränkt)

Address: Floningweg 16, 12107 Berlin, Germany

Contact person's name, position, and contact details: Felix Geilert, info@radiantscience.io

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in order to provide the Company Services as detailed in the Agreement.

Description of Transfer

Categories of Data Subjects:

Callers and Patients of the Customer or End Customer, and the Customer's staff and other Authorised Users.

Categories of Customer Personal Data transferred:

Patient and Caller name, voice, phone number and contact details, date of birth, appointment details, insurance and payment details provided by the Caller, the reason for the call and any health information disclosed during the call, and patient and appointment information retrieved from the Customer's calendar, practice management or electronic health record system to handle the call. Name, email address and role of Authorised Users.

Sensitive Data transferred (if applicable):

Yes, data related to patient health will be processed. Appropriate organisational, contractual and technical security measures will be implemented.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Customer Personal Data may be transferred on a continuous basis until it is deleted in accordance with the DPA.

Nature of the processing:

The Data Processing of the Personal Data is conducted for delivering Company Services outlined in the Agreement and shall include, but shall not be limited to, the following types of processing:

- collection;
- recording;

- organisation;
- structuring;
- storage;
- adaption or alteration;
- retrieval;
- consultation;
- use;
- disclosure by transmission, dissemination, or otherwise making available;
- alignment or combination;
- restriction;
- anonymisation;
- erasure; or
- Destruction.

Purpose(s) of the data transfer and further processing:

Company shall process the Customer Personal Data in order to provide the Company Services as detailed in the Agreement and Order Form.

The Data Processing will last for the duration of the Agreement and for any such period after the expiry or termination of such agreements to allow Company to comply with its legal obligations and return or delete the Customer Personal Data in accordance with this DPA.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

As set out in Sections 8 and 14: Call Content for the duration of the Agreement or the shorter period the Customer selects, then anonymised and deleted; other Customer Personal Data for the duration of the Agreement, then deleted within thirty (30) days of the Cessation Date; backups age out within seven (7) further days.

For transfers to (Sub)-processors, also specify the subject matter, nature, and duration of the processing

As above.

Annex II

All Sub-Processors are included in the [Subprocessors list](#).

Annex III

All technical and organisation measures are included in the [Technical and Organisational Measures document](#).