

This is a previous version, superseded on 14 Oct 2026. [View the current version.](#)

LEGAL

Data processing agreement

LAST UPDATED · 18 SEP 2026

Radiant Science UG

16 Floningweg, Berlin, 12107, Germany

Annex A: Data Processing Agreement

This Data Processing Agreement ("DPA") is incorporated into and forms part of the Company Terms and Conditions ("Agreement") between the Customer using the Company Services and Radiant Science UG ("The Company"). By accepting the Agreement, or by accessing or using the Company Services, the Customer agrees to this DPA on behalf of itself and its authorised users.

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 and with the 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) In the event of a conflict between the terms of this DPA and the Agreement, the DPA terms shall prevail with respect to the Processing of Customer Personal Data.

(E) Annex I and II are integral to this DPA and provide details about the Processing activities.

Definitions

“Agreement”: means the Company Terms & Conditions accepted by the Customer at login, including this DPA and all Schedules.

“Applicable Data Protection Law”: covers any applicable legislative or regulatory regime enacted by a recognised government, or governmental or administrative entity with the purpose of protecting the privacy rights of natural persons or households consisting of natural persons, including but not limited to: EU and the UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

“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.

“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.

“Contracted Processor”: means a Subprocessor of data.

“Data Controller” / “Controller”: shall mean the Customer that makes Customer Personal Data available to the Company.

“Company” / “Processor”: shall mean the entity providing the Services to the Customer, namely Radiant Science UG.

“EEA”: means the European Economic Area.

“EU Data Protection Laws”: means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii)

“Services”: means Company Services provided under the Agreement and this DPA.

“Subprocessor”: means any person appointed by or on behalf of the Data Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

“UK Data Protection Laws” means the UK GDPR, UK Data Protection Act 2018 and all other UK laws and regulations that apply to the processing of personal data.

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 GDPR, and their cognate terms shall be construed accordingly.

Company Restrictions and Responsibilities

1. Company shall, in delivering Services: (a) comply with all applicable Data Protection Laws, including UK GDPR and UK Data Protection Laws in the Processing of Customer Personal Data; (b) not Process Customer Personal Data other than as required to provide Company Services or on the Customer's documented instructions.
2. In the event the Company reasonably believes that an instruction issued by the Customer would violate any Applicable Data Protection Law, the Company shall promptly notify the Customer.
3. 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.
4. 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 the Applicable Data Protection Law; (c) and/or comply with all requests from a supervisory authority, including but not limited to in the event of an investigation.
5. Additional Company measures on handling of Customer Personal Data are outlined in an updated version of the Company Data Policy Guidelines. <https://www.radiantscience.io/privacy>

Customer Restrictions and Responsibilities

1. The Customer undertakes that it will ensure that its instructions, its use, the Customer Personal Data it makes subject to the Company Services and any other processing of Personal Data provided by the Company will comply with all Applicable Data Protection Laws, regulations, and rules applicable in relation to the Data made available by the Customer.
2. The Customer will be 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. Complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data (EU and UK Data Protection Law), including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes);
 3. Ensuring the Customer has the right to transfer, or provide access to, the Customer Personal Data to Company for Processing in accordance with the terms of the Agreement (including this DPA);
 4. Ensuring that instructions to Company regarding the processing of Personal Data comply with applicable laws, including Data Protection Laws;
 5. Informing Company without undue delay if the Customer is not able to comply with the Customer's responsibilities under this section or applicable Data Protection Laws.

3. The Customer will also ensure that the processing of Personal Data in accordance with its instructions will not cause or result in the Company or Customer breaching any laws, rules, or regulations.
4. The Customer undertakes that it will use the Company's services in compliance with the applicable laws and regulations, including obtaining lawful consent as required by the applicable laws. The Customer assumes full liability for collecting and processing Customer Personal Data in compliance with the applicable laws.
5. The Customer instructs the Company to process Customer Personal Data.
6. The Customer warrants that it has legal grounds under the Data Protection Legislation to process Personal Data for all Data Subjects whose Personal Data is processed by Company as part of the provision of the Services.
7. The Customer will promptly notify Company where it becomes aware that any Personal Data which is processed as part of the provision of the Services is inaccurate, out-of-date or incomplete and will promptly provide Company with correct, up-to-date and full Personal Data in that event.
8. The Parties each acknowledge that the subject matter, duration of processing, nature, and purpose of processing, categories of Data Subjects, and the types of Personal Data being processed are as detailed in Annex I, II, and III to this Agreement.

Company Personnel

Company shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Company 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, 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. 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 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.

Company 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.
3. 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. Customer may reasonably object to Company's use of a new Sub-Processor (e.g., if making Personal Data available to the Sub-Processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Company promptly in writing within fourteen (14) business days after receipt of Company's notice.

5. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-Processor, as permitted in the preceding sentence, Company will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening Customer. If 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 Company without the use of the objected-to new Sub-Processor by providing written notice to Company. Company will not refund 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.

Company Data Subject Rights

1. Taking into account the nature of the Processing, 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 the Data Protection Laws.
2. Company shall: (a) Promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; (b) Ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Company is subject, in which case Company shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before Company responds to the request.

Company 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; as part of the notification under Section of this DPA, to the extent reasonably available at the time of notice;
 2. Provide 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, and the risks to affected Data Subjects; promptly update the Customer as additional relevant information becomes available;
 3. Take all actions as may be required by Applicable Data Protection Law;
 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.

Company Data Protection Impact Assessment and Prior Consultation

Company shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, 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 Contracted Processors.

Company Deletion or Return of Customer Personal Data

Subject to this section, Company shall promptly and in any event within thirty (30) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the “Cessation Date”), delete and/or procure the deletion of all copies of Customer Personal Data except as required by Company to satisfy its business or to the extent Applicable Data Protection Laws or other applicable legal or regulatory requirements require storage of the Customer Personal Data for a longer period of time, the retention of the Customer Personal Data is necessary to resolve a dispute between the parties or the retention of the Customer Personal Data is necessary to combat harmful use of the Services. Customer Personal Data held in rolling database backups is not used or restored and ages out within seven (7) further days.

Company Audit Rights

1. Subject to this section, 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 the Personal Data by the 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 Law.
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. Customer will pay any reasonably incurred costs and expenses incurred by Company in the event Customer performs and audit that is not (a) required by Applicable Data Protection Laws, 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 Applicable Data Protection Law.

Company Data Transfers

1. 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 Data Processor.
2. The Customer provides the Company with general written authorization to transfer Personal Data outside of the EEA&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.

General Terms

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.

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 German Law. Each party irrevocably agrees that the Berlin, German courts 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.

Liability

- 1 . The liability of each party under this Agreement is subject to the exclusions and limitations of liability set out in the Agreement.
- 2 . The Data Controller warrants that it indemnifies, and shall keep indemnified, Data Processor against any liability, costs, expenses, losses, claims, or proceedings whatsoever arising under any statute, law, regulation, or at common law or for breach of contract arising out of, in connection with any act, omission or default of the Data Processor, its staff, agents or sub-contractors in relation to the Data, except in so far as such damages or injury shall be due to any gross negligence of Data Processor.

IN WITNESS WHEREOF, this DPA takes effect on the date the Customer first accepts the Agreement or accesses the Company Services, whichever is earlier.

Annex I

List of Parties

Data Controller ("The Customer")

Name: As provided by Customer during account registration on the Radiant Science platform.

Address: As provided by Customer during account registration on the Radiant Science platform.

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

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

Address: 16 Floningweg, Berlin, 12107, 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 Customer Personal Data transferred:

Patient name, patient voice, patient contact details, patient insurance and payment details, patient's medical history, diagnoses, medications, treatment plans, immunisation dates, allergies, radiology images, and laboratory and test results.

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;
- 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:

For the duration of the Agreement until deletion in accordance with the provisions of the DPA.

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

As above.

Annex II

All subprocessors are included in the [Subprocessors list](#).

Annex III

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