DATA PROCESSING AGREEMENT

ConnectHEOR Limited

Registered office: 5 St. John's Lane, London, England EC1M 4BH, United Kingdom

Document Control

Document title	Data Processing Agreement Template
Company	ConnectHEOR Limited
Registered office	5 St. John's Lane, London, England EC1M 4BH, United Kingdom
Purpose	Website and audit-ready DPA template for clients and prospective clients
Privacy contact	privacy@connectheor.com

1. Introduction and Parties

This Data Processing Agreement ("DPA") forms part of and is incorporated into the agreement, order form, statement of work, terms of use, master services agreement, professional services agreement, or any other written or electronic agreement governing the provision of services between the parties (the "Agreement").

This DPA is entered into by and between:

- ConnectHEOR Limited, a company incorporated in England and Wales with its registered office at 5 St. John's Lane, London, England EC1M 4BH, United Kingdom ("Processor", "ConnectHEOR", "we", "us" or "our"); and
- the customer, client or entity identified in the applicable Agreement or order document ("Controller", "Customer", "you" or "your").

The Controller and Processor are referred to individually as a "Party" and together as the "Parties". This DPA applies where ConnectHEOR processes Personal Data on behalf of the Controller in the course of providing services under the Agreement.

2. Purpose and Scope

The purpose of this DPA is to set out the parties' respective rights and obligations regarding the Processing of Personal Data and to support compliance with Applicable Data Protection Laws. This DPA applies only to Personal Data processed by ConnectHEOR as Processor on behalf of the Controller.

Where there is a conflict between this DPA and the Agreement in relation to the Processing of Personal Data, this DPA shall prevail to the extent of that conflict. Where Applicable Data Protection Laws impose stricter requirements, those laws shall prevail.

3. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below. Terms not defined in this DPA shall have the meaning given to them in Applicable Data Protection Laws or the Agreement.

Term	Meaning
Applicable Data Protection Laws	all applicable privacy and data protection laws and regulations relating to the Processing of Personal Data, including the UK GDPR, EU GDPR, the Data Protection Act

	2018, and any other privacy or data protection legislation applicable to the parties or the services.
Controller	the entity that determines the purposes and means of Processing Personal Data.
Processor	the entity that Processes Personal Data on behalf of the Controller.
Data Subject	an identified or identifiable natural person to whom Personal Data relates.
Personal Data	any information relating to an identified or identifiable natural person processed by Processor on behalf of Controller under the Agreement.
Processing	any operation or set of operations performed on Personal Data, including collection, recording, storage, use, analysis, disclosure, restriction, erasure or destruction.
Personal Data Breach	a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
Sub-Processor	any third party engaged by Processor to Process Personal Data on behalf of Controller.
SCCs	the European Commission Standard Contractual Clauses for international transfers of Personal Data, as updated or replaced from time to time.
UK Addendum	the UK International Data Transfer Addendum or any replacement mechanism approved by the UK Information Commissioner or applicable UK authority.

4. Roles of the Parties

- The Parties acknowledge and agree that, unless otherwise specified in the Agreement, the Customer acts as Controller and ConnectHEOR acts as Processor in respect of Personal Data processed under this DPA.
- Controller is responsible for determining the purposes and means of Processing and for ensuring that it has a lawful basis for providing Personal Data to Processor.
- Processor shall Process Personal Data only on behalf of Controller and in accordance with Controller's documented instructions, including the Agreement, applicable statements of work, and this DPA.

5. Documented Instructions

- Processor shall Process Personal Data only for the purposes of providing the services and only in accordance with documented instructions from Controller.
- Processor shall promptly inform Controller if, in Processor's reasonable opinion, an instruction infringes Applicable Data Protection Laws, unless prohibited from doing so by applicable law.
- Processor shall not sell Personal Data, share Personal Data for advertising purposes, or Process Personal Data for its own independent purposes.

6. Controller Obligations

- Controller shall ensure that all Personal Data provided to Processor has been collected and transferred lawfully.
- Controller shall provide all required notices to Data Subjects and obtain consents where required.

- Controller shall ensure that its Processing instructions are lawful, complete, accurate, and proportionate to the services.
- Controller shall be responsible for responding to Data Subject requests, unless the parties agree otherwise in writing.

7. Processor Obligations

- Processor shall comply with Applicable Data Protection Laws applicable to it as Processor.
- Processor shall ensure that persons authorized to Process Personal Data are subject to appropriate confidentiality obligations.
- Processor shall implement appropriate technical and organizational measures to protect Personal Data.
- Processor shall assist Controller, taking into account the nature of Processing and information available to Processor, with Controller's compliance obligations under Applicable Data Protection Laws.

8. Confidentiality

- Processor shall treat Personal Data as confidential and shall not disclose it except as permitted under the Agreement, this DPA, Controller's instructions, or applicable law.
- Processor shall ensure that employees, contractors, and other authorized personnel who access Personal Data are informed of the confidential nature of the data and are bound by confidentiality obligations.
- Confidentiality obligations shall continue after termination of the relevant employment, engagement, Agreement, or DPA.

9. Security Measures

- Processor shall maintain appropriate technical and organizational security measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.
- Such measures shall take into account the state of the art, cost of implementation, nature, scope, context and purposes of Processing, and the risk to Data Subjects.
- Processor shall regularly review and, where appropriate, update its security measures.

9.1 Indicative Technical and Organizational Measures

Control Area	Measure
Access control	Role-based access, least privilege access, user authentication, access reviews, and removal of access when no longer required.
Authentication	Strong password standards and multi-factor authentication where available and appropriate.
Encryption	Encryption of Personal Data in transit and at rest where appropriate, including use of recognized encryption standards.
Endpoint security	Anti-malware, endpoint protection, device configuration controls, and secure screen-locking practices.
Patch management	Timely application of security patches and updates for systems used to process Personal Data.
Backup and recovery	Backup processes and recovery procedures designed to support availability and resilience.
Awareness and training	Privacy, security, and confidentiality awareness for personnel

	with access to Personal Data.
Incident response	Procedures for identifying, managing, investigating, mitigating, and notifying relevant parties of security incidents.
Physical security	Reasonable physical safeguards for offices, equipment, and devices used to Process Personal Data.
Vendor controls	Due diligence and contractual controls for Sub-Processors that Process Personal Data.

10. Sub-Processors

- Controller provides general authorization for Processor to engage Sub-Processors where necessary to provide the services.
- Processor shall enter into written agreements with Sub-Processors imposing data protection obligations that are no less protective than those required under this DPA, to the extent applicable to the nature of services provided by the Sub-Processor.
- Processor shall remain responsible to Controller for the performance of its Sub-Processors' obligations relating to the Processing of Personal Data.
- Processor shall provide reasonable information regarding Sub-Processors upon request, subject to confidentiality and security restrictions.

11. Data Subject Rights

- Taking into account the nature of Processing, Processor shall provide reasonable assistance to Controller in responding to Data Subject requests relating to access, rectification, erasure, restriction, portability, objection, and other rights under Applicable Data Protection Laws.
- If Processor receives a Data Subject request directly, Processor shall promptly notify Controller unless legally prohibited from doing so. Processor shall not respond to the request except on Controller's documented instructions or as required by law.

12. Personal Data Breach Notification

- Processor shall notify Controller without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of Controller.
- The notification shall include, where available, the nature of the breach, categories and approximate number of affected Data Subjects and records, likely consequences, measures taken or proposed to address the breach, and contact details for follow-up.
- Processor shall cooperate reasonably with Controller in investigating, mitigating, remediating, and documenting the Personal Data Breach.

13. Assistance with Compliance

- Processor shall provide reasonable assistance to Controller, taking into account the nature of Processing and information available to Processor, with Controller's obligations relating to security, breach notification, data protection impact assessments, prior consultation with supervisory authorities, and records of Processing where applicable.
- Any assistance requiring significant additional effort may be subject to reasonable fees or terms agreed between the Parties, unless otherwise required by law or the Agreement.

14. International Transfers

- Processor shall not transfer Personal Data outside the United Kingdom or European Economic Area unless appropriate safeguards are in place as required by Applicable Data Protection Laws.
- Where required, the Parties shall use appropriate transfer mechanisms, including the SCCs, the UK Addendum, adequacy decisions, or other lawful mechanisms recognized under Applicable Data Protection Laws.
- Where SCCs or the UK Addendum apply, they shall be incorporated into this DPA by reference and shall prevail to the extent of any conflict relating to international transfers.

15. Records and Audit Rights

- Processor shall make available to Controller information reasonably necessary to demonstrate compliance with this DPA.
- Where required by Applicable Data Protection Laws, Processor shall allow for and reasonably contribute to audits or inspections conducted by Controller or an independent auditor mandated by Controller.
- Audits shall be subject to reasonable notice, confidentiality obligations, security requirements, and measures to avoid unnecessary disruption to Processor's business operations.
- Controller shall not access information relating to other customers, confidential business information, or security-sensitive information beyond what is reasonably necessary to verify compliance.

16. Return or Deletion of Personal Data

- Upon termination or expiry of the Agreement, or upon Controller's written instruction, Processor shall return or delete Personal Data processed on behalf of Controller, unless retention is required by applicable law.
- Where retention is required by law, Processor shall continue to protect the retained Personal Data in accordance with this DPA and shall not Process it except as required by law.
- Processor may retain backup copies for a limited period in accordance with its ordinary backup and retention procedures, provided such copies remain protected and are not actively processed except for restoration, legal compliance, or security purposes.

17. De-identified or Aggregated Data

- To the extent permitted by the Agreement and Applicable Data Protection Laws, Processor may create and use anonymized, aggregated, or de-identified information that does not identify Controller, Data Subjects, or any individual, provided such information cannot reasonably be used to re-identify Data Subjects.

18. Liability

- Each Party shall be responsible for its own compliance with Applicable Data Protection Laws.
- Liability arising under or in connection with this DPA shall be governed by the limitation of liability and related provisions set out in the Agreement, unless otherwise required by Applicable Data Protection Laws.

19. Term and Termination

- This DPA shall commence on the effective date of the Agreement and shall remain in force for as long as Processor Processes Personal Data on behalf of Controller.

- Termination or expiry of the Agreement shall not affect rights and obligations that, by their nature, are intended to survive, including confidentiality, return or deletion, and legal retention obligations.

20. Governing Law

- This DPA shall be governed by the governing law specified in the Agreement. If the Agreement does not specify a governing law, this DPA shall be governed by the laws of England and Wales, unless Applicable Data Protection Laws require otherwise.

Annex 1 - Details of Processing

Item	Description
Subject matter of Processing	Processing of Personal Data in connection with the provision of healthcare research, HEOR, RWE, evidence strategy, consulting, analytics, advisory, and related professional services under the Agreement.
Duration of Processing	For the duration of the Agreement and thereafter only as required for lawful retention, audit support, dispute resolution, backup, or legal compliance.
Nature of Processing	Collection, receipt, recording, organization, structuring, storage, retrieval, consultation, analysis, use, disclosure as instructed, restriction, return, deletion, and destruction.
Purpose of Processing	To enable ConnectHEOR to provide the services described in the Agreement, applicable statement of work, order form, or project documentation.
Categories of Data Subjects	Client representatives, healthcare professionals, key opinion leaders, research participants where applicable, suppliers, contractors, business contacts, and other individuals whose Personal Data is provided by Controller.
Categories of Personal Data	Name, title, role, professional contact details, employer or organization, specialty, professional background, communications, project information, research-related responses or inputs, payment or contracting details where applicable, and any other Personal Data provided by Controller.
Special Category Data	Special category data should not be provided unless expressly required under the Agreement or project documentation and supported by an appropriate lawful basis and safeguards.
Frequency of Processing	Continuous or as required for the provision of services under the Agreement.
Retention	As specified in the Agreement, statement of work, Controller instructions, or applicable retention/legal requirements.

Annex 2 - International Transfer Safeguards

Where Personal Data is transferred internationally and Applicable Data Protection Laws require a transfer mechanism, the Parties shall rely on the applicable SCCs, the UK Addendum, adequacy decisions, or other lawful transfer mechanisms. The Parties shall cooperate reasonably to complete any transfer impact assessment or supplementary measures assessment required by Applicable Data Protection Laws.

Annex 3 - Sub-Processor Information

Processor shall maintain reasonable information regarding Sub-Processors used to provide the services. Sub-Processor information may be provided upon request or made available through a separate Sub-Processor list, subject to confidentiality and security considerations.

Execution

This DPA may be executed by signature, electronic acceptance, incorporation into the Agreement, or other method agreed by the Parties.

For Controller	
	For Processor: ConnectHEOR Limited
Name / Title / Date	
Signature	

Company details for notices: ConnectHEOR Limited, 5 St. John's Lane, London, England EC1M 4BH, United Kingdom. Privacy contact: privacy@connectheor.com.