

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) forms part of and is incorporated into the Exa [Terms of Service, Master Subscription Agreement](#) and any other terms of service or agreements that expressly incorporate it (the “**Agreement**”) between Exa Labs, Inc. (“**Exa**”) and the relevant business customer that is party to the Agreement (“**Customer**”) (together, the “**Parties**”).

This DPA sets forth Customer’s instructions for the processing of Personal Data in connection with the services provided under the Agreement (the “**Services**”) and the rights and obligations of both Parties. Except as expressly set forth in this DPA, the Agreement shall remain unmodified and in full force and effect. In the event of any conflicts between this DPA and the Agreement, this DPA will govern to the extent of the conflict.

1. **Definitions.** For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalized terms used but not defined in this DPA shall have the meanings given in the Agreement. All other terms in this DPA not otherwise defined in the Agreement shall have the corresponding meanings given to them in Privacy Laws.
 - a. “**Controller to Processor Clauses**” means (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 2 (Controller to Processor) (“**EU SCCs**”); and (ii) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner (“**UK Addendum**”), in each case as amended, updated or replaced from time to time.
 - b. “**EU/UK Privacy Laws**” means, as applicable: (i) the General Data Protection Regulation 2016/679 (the “**GDPR**”); (ii) the Privacy and Electronic Communications Directive 2002/58/EC; (iii) the UK Data Protection Act 2018, the UK General Data Protection Regulation as defined by the UK Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the UK Data Protection Act 2018, the “**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003; and (iv) any relevant law, directive, order, rule, regulation or other binding instrument which implements any of the above, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.
 - c. “**Personal Data**” means any information Exa processes on behalf of Customer to provide the Services that is defined as “personal data” or “personal information” under any Privacy Law.
 - d. “**Privacy Laws**” means, as applicable, EU/UK Privacy Laws, US Privacy Laws and any similar law of any other jurisdiction which relates to data protection, privacy or the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.
 - e. “**Processor to Processor Clauses**” means (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of personal data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 3 (Processor to Processor); and (ii) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time.

- f. **“Third Country”** means any country or territory outside of the scope of the data protection laws of the European Economic Area or the UK, as relevant, excluding countries or territories approved as providing adequate protection for Personal Data by the relevant competent authority from time to time.
 - g. **“US Privacy Laws”** means, as applicable, the California Consumer Privacy Act and any similar law of any other state related to the processing of Personal Data.
- 2. **Amendments.** The Parties agree to negotiate in good faith modifications to this DPA if changes are required for Exa to continue to process the Personal Data as contemplated by the Agreement or this DPA in compliance with Privacy Laws, or to address the legal interpretation of the Privacy Laws.
- 3. **Roles of the Parties.** The Parties acknowledge that for purposes of Privacy Laws, Customer is the controller, business, or any similar term provided under Privacy Laws, and Exa is the service provider, processor, or any similar term provided under Privacy Laws.
- 4. **Details of Processing.** The Parties agree that the details of processing are as described in Annex 1.
- 5. **Customer Obligations.** Customer shall comply with all Privacy Laws in providing Personal Data to Exa in connection with the Services. Customer represents and warrants that: (a) the Privacy Laws applicable to Customer do not prevent Exa from fulfilling the instructions received from Customer and performing Exa’s obligations under this DPA; (b) all Personal Data was collected and at all times processed and maintained by or on behalf of Customer in compliance with all Privacy Laws, including with respect to any obligations to provide notice to and/or obtain consent from individuals; and (c) Customer has a lawful basis for disclosing the Personal Data to Exa and enabling Exa to process the Personal Data as set out in this DPA. Customer shall notify Exa without undue delay if Customer makes a determination that the processing of Personal Data under the Agreement does not or will not comply with Privacy Laws, in which case, Exa shall not be required to continue processing such Personal Data.
- 6. **Processing of Personal Data.** In processing Personal Data under the Agreement, Exa shall:
 - a. only process Personal Data on documented instructions from Customer, for the limited and specific purpose described in Annex 1, and at all times in compliance with Privacy Laws, unless required to process such Personal Data by applicable law to which Exa is subject; in such a case, Exa shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - b. notify Customer (i) without undue delay if it makes a determination that it can no longer meet its obligations under applicable US Privacy Laws, and (ii) immediately if Exa, in its opinion, on the instruction of Customer, infringes applicable EU/UK Privacy Laws;
 - c. to the extent required by US Privacy Laws, and upon reasonable written notice that Customer reasonably believes Exa is using Personal Data in violation of Privacy Laws or this DPA, grant Customer the right to take reasonable and appropriate steps to help ensure that Exa uses the Personal Data in a manner consistent with Customer’s obligations under Privacy Laws, and stop and remediate any unauthorized use of the Personal Data; and
 - d. require that each employee or other person processing Personal Data is subject to an appropriate duty of confidentiality with respect to such Personal Data.

7. **Anonymized Data.** Exa may aggregate and/or anonymize Personal Data such that it no longer constitutes Personal Data under Privacy Laws and process such data for its own purposes. To the extent Exa receives de-identified data (as such term is defined under applicable US Privacy Laws) from Customer, Exa shall: (a) take commercially reasonable measures to ensure that the data cannot be associated with an identified or identifiable individual; (b) publicly commit to maintain and use the data only in a de-identified form and not attempt to re-identify the data; and (c) otherwise comply with applicable US Privacy Laws with respect to such de-identified data.
8. **Prohibitions.** To the extent required by applicable US Privacy Laws, and except to the extent permitted by such US Privacy Laws, Exa is prohibited from:
 - a. selling the Personal Data or sharing the Personal Data for cross-context behavioral advertising purposes;
 - b. retaining, using, or disclosing the Personal Data outside of the direct business relationship between Exa and Customer and for any purpose other than for the specific purpose of performing the Services; and
 - c. combining the Personal Data received from, or on behalf of, Customer with any Personal Data that may be collected from Exa's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Privacy Laws.
9. **Use of Subcontractors.** To the extent Exa engages any subcontractors to process Personal Data on its behalf:
 - a. Customer hereby grants Exa general written authorization to engage the subcontractors available at <https://docs.exa.ai/reference/security>, subject to the requirements of this Section 9.
 - b. If Exa appoints a new subcontractor or intends to make any changes concerning the addition or replacement of any subcontractor, it shall provide Customer with prior written notice by updating the list of subcontractors available at <https://docs.exa.ai/reference/security>, which Customer shall periodically check for updates. For a period of 10 business days after any such update, Customer can object to the appointment or replacement on reasonable and documented grounds related to the confidentiality or security of Personal Data or the subcontractor's compliance with Privacy Laws (and if Customer does not so object, Exa may proceed with the appointment or replacement).
 - c. Exa shall engage subcontractors only pursuant to a written agreement that contains obligations on the subcontractor which are no less onerous on the relevant subcontractor than the obligations on Exa under this DPA.
 - d. In the event Exa engages a subcontractor to carry out specific processing activities on behalf of Customer pursuant to EU/UK Privacy Laws, where that subcontractor fails to fulfil its obligations, Exa shall remain fully liable under applicable EU/UK Privacy Laws to Customer for the performance of that subcontractor's obligations.
10. **Assistance.** To the extent required by Privacy Laws, and taking into account the nature of the processing, Exa shall, in relation to the processing of Personal Data and to enable Customer to comply with its obligations which arise as a result thereof, provide reasonable assistance to Customer, through appropriate technical and organizational measures, in:

- a. responding to requests from individuals pursuant to their rights under Privacy Laws, including by providing, deleting or correcting the relevant Personal Data, or by enabling Customer to do the same, insofar as this is possible;
 - b. implementing reasonable security procedures and practices appropriate to the nature of the Personal Data to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure;
 - c. notifying relevant competent authorities and/or affected individuals of Personal Data breaches;
 - d. conducting data protection impact assessments and, if required, prior consultation with relevant competent authorities; and
 - e. entering into this DPA.
11. **Security Measures.** Exa shall, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purpose of the processing, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk, as set out in Annex 3, or otherwise agreed and documented between Customer and Exa from time to time. To the extent required by Privacy Laws, Exa shall without undue delay notify Customer in writing of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, with further information about the breach provided in phases as more details become available.
12. **Access and Audits.** Upon reasonable request of Customer, Exa shall make available to Customer such information in its possession as is reasonably necessary to demonstrate Exa's compliance with its obligations under this DPA, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer and reasonably accepted by Exa. Customer shall be permitted to conduct such an assessment no more than once every 12 months, upon 30 days' advance written notice to Exa, and only after the Parties come to agreement on the scope of the audit and the auditor is bound by a duty of confidentiality. As an alternative to an audit performed by or at the direction of Customer, to the extent permitted by Privacy Laws, Exa may arrange for a qualified and independent auditor to conduct, at Exa's expense, an assessment of Exa's policies and technical and organizational measures in support of its obligations under Privacy Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessment, and will provide a report of such assessment to Customer upon reasonable request. Notwithstanding the foregoing, in no event shall Exa be required to give Customer access to information, facilities or systems to the extent doing so would cause Exa to be in violation of confidentiality obligations owed to other customers or its legal obligations.
13. **Deletion of Personal Data.** At Customer's written direction, Exa shall delete or return all Personal Data to Customer as requested at the end of the provision of the Services, unless retention of the Personal Data is required by law.
14. **Data Transfers.** To the extent Exa processes Personal Data subject to EU/UK Privacy Laws in a Third Country, and it is acting as data importer, Exa shall comply with the data importer's obligations and Customer shall comply with the data exporter's obligations set out in the Controller to Processor Clauses, which are hereby incorporated into and form part of this DPA, and:
 - a. for the purposes of Annex I or Part 1 (as relevant), Customer is a controller and Exa is a processor, and the parties, contact person's details and processing details set out in the

Agreement, this DPA and Annex 1 shall apply and the Start Date is the effective date of the Agreement;

- b. if applicable, for the purposes of Part 1 of the UK Addendum, the relevant Addendum EU SCCs (as such term is defined in the UK Addendum) are the EU SCCs as incorporated into this DPA by virtue of this Section 14;
- c. for the purposes of Annex II or Part 1 (as relevant), the technical and organizational security measures, and the technical and organizational measures taken by Exa to assist Customer, as each are set out in Annex 3, shall apply; and
- d. if applicable, for the purposes of: (i) Clause 9, Option 2 (“General written authorization”) is deemed to be selected and the notice period specified in Section 9 shall apply; (ii) Clause 11(a), the optional wording in relation to independent dispute resolution is deemed to be omitted; (iii) Clause 13 and Annex I.C, the competent supervisory authority shall be Ireland; (iv) Clauses 17 and 18, Option 1 is deemed to be selected and the governing law and the competent courts shall be Ireland; (v) Part 1, Exa as importer may terminate the UK Addendum pursuant to Section 19 of such UK Addendum.

Customer acknowledges and agrees that Exa may appoint an affiliate or third-party subcontractor to process the Personal Data in a Third Country, in which case, Exa shall execute the Processor to Processor Clauses with any relevant subcontractor (including affiliates) it appoints on behalf of Customer.

15. **Severability.** If any provision in this DPA is deemed by a court of competent jurisdiction or regulatory authority to be invalid, prohibited or unenforceable, such provision shall, as to the relevant jurisdiction, be ineffective to the extent of such prohibition or unenforceability but shall be valid and enforceable to the fullest extent permitted by law. The remainder of this DPA will remain in full force and effect, and will be modified to any extent necessary to give such force and effect to the remaining provisions, but only to such extent.

ANNEX 1

Details of Processing

Nature of the processing

Access, use, disclosure, storage and deletion of Personal Data by Exa in connection with its provision of the Services to Customer as set out in the Agreement.

Purpose(s) of the processing

The provision of the Services by Exa to Customer as set out in the Agreement.

Categories of individuals whose Personal Data is processed

Customer's authorized employees and contractors, and other categories of individuals as otherwise determined by Customer.

Categories of Personal Data processed

Name, email address and other account information of Customer's employees and contractors who are authorized to access the Services, or any Personal Data contained in User Input or Input submitted through the Services as determined by Customer.

Types of Personal Data subject to the processing that are considered "sensitive" or "special category" under Privacy Laws

No "sensitive" or "special category" data is intended to be processed.

Frequency (e.g. one-off or continuous) and duration of the processing

Relevant Personal Data is processed on a continuous basis, for the duration of the term of the Agreement and any post-termination retention period as set out in the Agreement.

The subject matter, nature and duration of processing carried out by any sub-processors authorized pursuant to Section 9 is as set out in this Annex 1 and in the list of subcontractors available at <https://docs.exa.ai/reference/security>.

ANNEX 2

Security Measures

1. **Physical Access Management.** Exa shall take, at a minimum, the following technical and organizational measures in order to establish the identity of the authorized persons and prevent unauthorized access to the Exa's premises and facilities in which the Personal Data are processed:
 - All entrances are locked and can only be accessed with the appropriate key / chip card / security code
 - Windows and doors are protected by an alarm system
 - All external visitors are required to present identification and are signed in by authorized staff
 - Video monitoring of visitors
 - Visitors are accompanied by Exa's personnel at all times
 - Full perimeter surveillance cameras
2. **System Entry Management.** Exa shall take, at a minimum, the following technical and organizational measures in order to prevent unauthorized access to the data processing systems:
 - Unique user authentication via user name and password for each network and system access required (default passwords changed at first login)
 - Use of firewalls
 - During idle times, user and administrator PCs are automatically locked
 - Concept of least privilege, allowing only the necessary access for users to accomplish their job function. Access above these least privileges requires appropriate authorization
 - IT access privileges are reviewed regularly (at least every quarter) by appropriate personnel
 - Network monitoring services in place 24 x 7 x 365 to detect unauthorized activities
 - Vulnerability scanning and remediation in place
 - Data center and website penetration testing program in place
3. **Data Access Management.** Exa shall take, at a minimum, the following technical and organizational measures in order to prevent unauthorized activities in the data processing systems outside the scope of any granted authorizations:
 - User and administrator access to the network is based on a role based access rights model. There is an authorization concept in place that grants access rights to data only on a "need to know" basis
 - Administration of user rights through system administrators
 - Number of administrators is reduced to the absolute minimum
 - IT governance & controls audits undertaken annually by external third party

- Internal control audits undertaken regularly
 - Network monitoring services in place 24 x 7 x 365 to detect unauthorized activities
4. **Onward Data Transfer.** Exa shall take, at a minimum, the following technical and organizational measures in order to ensure that Personal Data cannot be read, copied, altered or removed by unauthorized persons under their electronic transmission or during their transport or recording on data carriers and to guarantee that it is possible to examine and establish where Personal Data are or have had to be transmitted by data transmission equipment:
- Access requires user identification and authorisation
 - Use of e-mail encryption
 - Data transferred by Exa is transported and saved in encrypted form; the relevant areas of the data carriers are encrypted using data and hard drive encryption software
 - Data transferred by Exa is transferred in pseudonymized form
 - Data storage devices and paper documents are locked away when not in use (clean desk policy)
 - Physical transports are only performed with locked containers and/or guarded vehicles
 - Use of document shredders
 - Secure destruction processes in place to industry standards utilising specialized third party with disposal certificates produced to ensure limited data retention
 - The secure transfer modes and encryption methods are regularly updated, tested and kept state-of-the-art (*e.g.*, according to the recommendations in the data protection manual issued by the BSI (Federal Office for Information Security)) to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services
 - Third party secure off-site tape storage utilized
 - Secure communication session established via HTTPS and SFTP protocols across all applications / services
 - Encrypted certificates utilized for authentication between the web client and the web server across all websites
 - Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident and in general, for data portability
 - Measures for ensuring events logging
 - Measures for ensuring internal IT and IT security governance and management and measures for ensuring accountability
 - Measures for ensuring data quality
 - Measures for ensuring data minimisation

5. **Input Management.** Exa shall take, at a minimum, the following technical and organizational measures in order to ensure that it is subsequently possible to verify and establish whether and by whom Personal Data have been entered into data processing systems, altered or removed:
 - Access to electronic documents / applications is documented via auditable log files
 - Access to physical documents is documented via protocols
 - Protocolling input, modification and deletion of data by use of individual user names
6. **Instructions.** Exa shall take, at a minimum, the following technical and organizational measures in order to ensure that Personal Data which are processed on behalf of Exa can only be processed in compliance with Exa's instructions:
 - Clear and binding internal policies contain formalized instructions for data processing procedures
 - Unambiguous language in the underlying contracts
 - Careful selection of contractors, especially with regard to data security aspects
 - Internal monitoring of quality of service includes compliance with contractual arrangements
 - Regular audits by third parties include compliance with contractual arrangements
 - Regular staff training to ensure compliance with contractual arrangements and maintain awareness regarding data protection requirements
 - Secure destruction processes in place to industry standards utilising specialized third party with disposal certificates produced
 - Periodic risk assessments focus on how insider access is controlled and monitored
7. **Availability.** Exa shall take, at a minimum, the following technical and organizational measures in order to protect the data from accidental destruction or loss:
 - Appliances for the monitoring of temperature and humidity
 - Fire / smoke detectors and fire extinguishers in the areas where data is stored / processed
 - State-of-the-art firewall
 - Data recovery measures and emergency plan in place and regularly tested
 - Implementation of state-of-the-art backup methods such as: tape backup, data mirroring, and so on. Physical separation of the backup data; data stored in the archive is saved using redundant systems.
 - Uses a combination of full, differential, and cumulative backups to ensure data integrity and timely restoration
 - Backup tapes are securely stored both on-site and off-site to provide protection against disaster and efficient data recovery
 - To ensure an uninterrupted supply of power to the system, redundant power supply units are built into the systems wherever possible.

- Data is stored redundantly on multiple devices
- Integrity of stored data regularly verified using checksums
- Automated processes move data traffic away from affected area to uncompromised area in case of failure
- Preventative maintenance is performed to ensure continued operability of equipment

8. **Separation and Purpose.** Exa shall take, at a minimum, the following technical and organizational measures in order to ensure that data collected for different purposes are processed separately:

- Documents that are stored physically are stored separately for each Customer and the respective containers are clearly labelled
- Implementation of an authorization concept
- Strong isolation between guest virtual machines is maintained; Exas are prevented from accessing areas not assigned to them by filtering through the virtualization software
- A unique encryption key is created per Exa