leapwork

Data Processing Addendum

between

Entity described as "Leapwork" in the Agreement ("**Data Processor**"), and

Entity described as "Customer" in the Agreement ("**Data Controller**");

The Data Controller and the Data Processor are hereinafter individually referred to as a "**Party**" and jointly, the "**Parties**".

The Parties have concluded this Data Processing Addendum ("**DPA**"):

1. Introduction and Definitions

1.1 This DPA has been made in connection with and forms part of the End User License Agreement and/or Master Subscription Agreement (each, the "Agreement", as applicable) entered between the Data Controller and the Data Processor concerning the Data Processor's Offerings (as defined in the Agreement and to the extent applicable in the Order Form).

1.2 The Agreement governs the general terms relating to the Offerings provided by the Data Processor to the Data Controller, and this DPA governs the processing of personal data in connection with such Offerings. To the extent relating to data protection matters, this DPA shall prevail in the event of any conflict between this DPA and the Agreement or any other documents incorporated therein.

1.3 Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

1.4 Any reference to this DPA includes its Annexes and Appendices, which form an integral part of this DPA.

1.5 The Agreement remains confidential between the Parties. Sub-processors may be informed of the contents of this DPA only to the extent necessary for the performance of the Offerings and in accordance with the terms of this DPA.

1.6 Definitions

Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;
Data Protection Laws	means as applicable and binding on the Data Controller and Data Processor (i) in the United Kingdom the Data Protection Act 2018; and the GDPR, and/or any corresponding or equivalent national laws or regulations; (ii) in member states of the European Union (EU) and/or European Economic Area (EEA): the GDPR and all relevant EU and EEA member state laws or regulations giving effect to or corresponding with any of the GDPR; (III) in the United States the CCPA; and

(iv) any applicable laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;

GDPR	means the General Data Protection Regulation (EU) 2016/679;
CCPA	means the California Consumer Privacy Act of 2018, together with all regulations implementing or supplementing the same, to the extent applicable to Data Processor in its performance of the Offerings. Only to the extent Data Processor processes personal information of Californian residents that Data Controller provides or makes available to Data Processor in connection with the Offerings, the CCPA Addendum (Appendix C) will apply.
Protected Data	means personal data received from or on behalf of the Data Controller to the extent that it is processed by Data Processor on Data Controller's behalf in connection with the performance of Data Processor's obligations under the Agreement;
EU SCCs	means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, adopted by the European Commission decision (EU) 2021/914 of 4 June 2021;
UK SCCs	means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK ICO under S119A(1) Data Protection Act 2018 and in force March 21, 2022.

2. Personal Data and data processing activities

2.1 This DPA defines and governs the personal data, the data subjects, the purposes and the data processing activities that will be carried out by the Parties while performing the Agreement and other matters and obligations relating to the processing, as defined and stated in Annex 1 hereto. **Annexes 1-3** and **Appendices A-C** form part of both Parties' documentation obligations under Data Protection Laws and must always reflect the actual circumstances.

2.2 The Data Controller warrants and undertakes that the personal data has been collected, processed and transferred in accordance with GDPR and all other applicable Data Protection Laws.

3. Roles and instructions

3.1 The Data Processor is the data processor under applicable Data Protection Laws and processes personal Data on behalf of the Data Controller who is the data controller under applicable Data Protection Laws.

3.2 The Data Controller decides for which purposes and how the Data Processor may process the personal data.

3.3 The Data Processor may and shall process the personal data only pursuant to documented instructions from the Data Controller as set out in **Annexes 1-3** and **Appendices A-C**, or other written instructions unless required to do so Data Protection Laws to which the Data Processor is subject. In such a case, the Data Processor must inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.4 The Data Controller guarantees that the personal data transferred to the Data Processor is collected, processed and transferred in accordance with applicable Data Protection Laws, including but not limited to the legal grounds for processing and the requirement to provide data subjects with certain information.

3.5 The Data Processor must delete and/or dispose of personal data in all systems and files only upon instructions of the Data Controller.

4. Confidentiality

4.1 The personal data provided to the Data Processor by the Data Controller or otherwise obtained by the Data Processor in the course of carrying out the Offerings is confidential.

4.2 The Data Processor must ensure that only employees and other individuals who, at any given time, are required to process the personal data as part of their job have been authorised to do so.

4.3 The Data Processor must further ensure that the individuals authorised to process the Data Controller's personal data have undertaken a duty of confidentiality for all personal data to which they have access or that they are subject to an appropriate statutory duty of confidentiality.

5. Supporting the Rights of the Data Subjects

Considering the nature of processing and the information available to the Data Processor, the Data Processor shall implement appropriate technical and organizational measures to assist the Data Controller in the fulfilment of the Data Controller's legal obligations under Chapter III (Rights of Data Subjects) of GDPR.

6. Security

6.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity of the rights and freedom of natural persons, the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate for the risk, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data transmitted, stored or otherwise processed.

7. International Transfers of Personal Data

7.1 The Data Controller agrees that the Data Processor may transfer Protected Data to countries outside the EEA, the United Kingdom or to any international organisation(s) (an **International Recipient**), provided all transfers by Data Processor of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of this Agreement shall constitute the Data Controller's instructions with respect to transfers in accordance with Section 3.

7.2 If Data Controller transfers personal data to Data Processor from the European Economic Area (EEA), Switzerland, or the United Kingdom (UK), the Parties will apply one of the following to the extent an Appropriate Safeguard is legally required in descending order of preference, such that the item highest on the list that is applicable and available will automatically apply during the term of this Agreement: (i) a valid finding Adequacy Decision;

(ii) any mechanism, derogation, exemption, or exception that the Parties are able to invoke, such as the consent of the relevant data subjects or a derogation under Article 49 of the GDPR; or (iii) the applicable EU SCCs and/or UK SCCs pursuant to Appendices A-B. Nothing in the interpretations of this DPA is intended to conflict with either Party's rights or responsibilities under the EU SCCs or UK SCCs and, in the event of any such conflict, the EU SCCs or UK SCCs shall prevail, as applicable. To the extent a transfer mechanism other than the foregoing becomes reasonably available to the Parties after the effective date of this DPA, the Parties will consult with each other in good faith on whether to rely on such transfer mechanism in lieu of the applicable EU SCCs or UK SCCs.

7.3 Without prejudice to the generality of the foregoing, Data Controller agrees to the transfer of personal data to sub-processors outside of the UK or EEA pursuant to Section 8 and as further set out in Annex 3 or as otherwise notified to Data Controller by Data Processor pursuant to Section 8 below.

8. Sub-processors

8.1 Subject this section 8, the Data Processor has the Data Controller's general authorisation for the engagement of sub-processors without obtaining any further written, specific authorisation from the Data Controller. The Data Processor shall specifically inform in writing the Data Controller about the identity of any potential new sub-processor at least 7 (seven) days in advance, thereby giving the Data Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s).

8.2 If the Data Controller (acting reasonably) does not approve of a new sub-processor, the Data Controller may, within 7 (seven) days from the notification to the Data Controller, request that the Data Processor move the Protected Data to another sub-processor by email to privacy@leapwork.com. If a request is received from Data Controller within the time frame, the Data Processor shall, within a reasonable period of time following receipt of such request, use all reasonable endeavours to ensure that the relevant sub-processor does not process any further Protected Data, and help identify an alternative. If such a request is not received within this time frame, the new sub-processor shall be deemed to have been approved.

8.3 Further, it is a condition for the use of the sub-processor(s) that the Data Processor enters into a written agreement with the sub-processor stating the sub-processor's duty to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of applicable Data Protection Laws.

8.4 The Data Controller has approved the sub-processor(s) listed in Annex 3. The Data Processor shall continuously update Annex 3 with information on the sub-processor(s) approved by the Data Controller and share the updated Annex 3 with the Data Controller when changes are made.

9. Assistance to the Data Controller

9.1 Taking into account the nature of processing and the information available to the Data Processor, the Data Processor must assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, i.e. with regard to security measures, notification of supervisory authorities, notification of individuals, preparation of data protection impact assessments and prior consultation with supervisory authorities.

leapwork

10. Personal Data Breaches

10.1 In case of a Personal Data Breach relating to the Personal Data, the Data Processor shall notify the Data Controller without undue delay of when the Data Processor is made aware of the Personal Data Breach.

10.2 Taking into account the nature of processing as well as the information available to the Data Processor, following a personal data breach at the Data Processor, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's legal obligations in connection with the notification of personal data breaches to supervisory authorities and to data subjects.

10.3 Further, following a personal data breach at the Data Processor, taking into account the nature of processing as well as to the extent the information is available to the Data Processor, the Data Processor must use its best efforts to provide the Data Controller with the information stated in GDPR Article 33 without undue delay, to enable the Data Controller to comply with any statutory obligations.

10.4 If and to the extent that it is not possible to immediately provide the information mentioned under clauses 10.1 - 10.3, the information can be provided gradually but no later than 72 hours from when the Data Processor was made aware of the personal data breach.

11. Demonstration of compliance and audits

11.1 The Data Processor must upon written request make available to the Data Controller reasonable information necessary to demonstrate its compliance with the obligations stipulated in this DPA and applicable Data Protection Laws.

11.2 The Data Processor must allow for and contribute to audits, including inspections, conducted by the Data Controller, auditors mandated by the Data Controller, or public authorities in competent jurisdictions. The auditor in question must be subject to confidentiality, either contractually or by law.

11.3 The above clauses 11.1 and 11.2 shall not be applicable if the Data Processor can present an audit report produced by an external qualified auditor and no older than 12 months without any material remarks regarding GDPR compliance and the compliance with this DPA.

12. Information

12.1 The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes any applicable Data Protection Laws.

12.2 To the extent relevant, the Data Controller must inform the Data Processor of any legislation other than the GDPR, as for example any special, local requirements for the storage of Personal Data in the country of the Data Controller. If such special legislation flows down and imposes additional obligations on the Data Processor beyond GDPR, the Parties must discuss the additionally required adaption to systems and processes and the payment for any such adaption.

leapwork

13. Liability

13.1 To the maximum extent allowed by applicable laws, the Parties' liabilities arising out of or in connection with this DPA, whether in contract, tort or under any other theory of liability, will be subject to any aggregate limitation of liability and any exclusions of damages set forth in the Agreement, and any reference to the liability of the Parties shall mean the aggregate liability under the Agreement and this DPA together.

13.2 Data Processor will not be liable for any claim brought by a data subject arising from any action by Data Processor to the extent that such action resulted directly from the Data Controller's instructions. In such case, the Data controller shall indemnify, keep indemnified and defend at its own expense Data Processor against all associated costs, claims, damages or expenses incurred by Data Processor.

13.3 Each Party shall on their own be liable for any administrative fines that a supervising authority may impose due to their processing.

14. Severability

14.1 If any of the clauses of this DPA is held invalid, this shall not affect the validity of the remaining DPA.

15. Term and termination

15.1 This DPA shall remain in force for as long as the duration of the Agreement or longer, if terms in the Agreement, this DPA or requirements set out in applicable legislation require so.

15.2 This DPA shall terminate without notice at the time of termination/expiry of the Agreement.

15.3 This DPA applies to all processing of personal data carried out by the Data Processor in connection with the provision of the Offerings and to all personal data held by the Data Processor whether held on the date of this DPA or held or received after its expiry or termination. Hence, this DPA, including relevant provisions of the Agreement, will survive for as long as the Data Processor processes personal data, also if such processing takes place after termination of this DPA.

15.4 After the end of the provision of the Offerings and at the termination of this DPA (whichever time is the latest), the Data Processor shall, at the discretion of the Data Controller, delete or return all existing copies of the personal data and delete all existing copies of the personal data processed on behalf of the Controller, except for any personal data that the Data Processor may be obligated to store according to mandatory laws (as applicable).

15.2 This clause 15 and the relevant references will survive any termination of this DPA.

16. Governing law and venue

16.1 This DPA and all non-contractual or other obligations arising out of or in connection with it are subject to the governing law and jurisdiction provisions of the Agreement, except with respect to (i) the EU SCCs, which shall be governed by the law of Denmark, and (ii) the UK SCCs, which shall be governed by the laws of England and Wales.

leapwork

17. Appendices

17.1 The following Appendices to this DPA constitute an integral part of the DPA:

Annex 1: Information about the processing operations
Annex 2: Minimum security requirements
Annex 3: List of sub-processors
Appendix A: EU SCCs
Appendix B: UK SCCs
Appendix C: CCPA Addendum

leapwork

ANNEX 1

Information about the processing operations

1. General

The Data Processor provides the Offerings under the Agreement, which may include software products and related services such as test automation, performance testing, AI-enabled features, support, analytics, and associated functionalities.

The Data Processor does not require the use of personal data for the intended use of the Offerings. However, depending on the Data Controller's use of the Offerings, Customer Data processed by the Data Processor may include personal data.

2. Data Subjects

The Data Processor processes personal data relating to the following categories of data subjects:

- the Data Controller's employees, contractors, or other users authorised to use the Offerings
- where applicable, the Data Controller's customers or end users, to the extent their data is included in Customer Data processed through the Offerings

3. Categories of personal data

3.1 Platform and User Data (always processed)

The Data Processor processes limited personal data necessary to provide access to and operate the Offerings, including:

- identification data (e.g. name, email address, phone number)
- user account and authentication data (e.g. login credentials, user IDs)
- technical data (e.g. IP address, device and session information)

3.2 Customer Data (processed depending on use)

Depending on the Data Controller's use of the Offerings, the Data Processor may process personal data contained in Customer Data submitted, uploaded, or generated by the Data Controller, including:

- data included in test automation scenarios and datasets
- application data processed or returned by the Data Controller's systems
- system-generated data such as logs, execution data, and analytics
- identifiers such as user IDs, tenant IDs, and system-generated identifiers

3.3 Additional Data for Performance Testing (Leapwork Performance)

Where the Data Controller uses Leapwork Performance (RUSH), Customer Data may additionally include:

- request and response data (e.g. API payloads, request bodies, response bodies)
- HTTP metadata (e.g. headers, cookies, query parameters)
- authentication-related data (e.g. authorization headers, session tokens, API keys)
- performance and execution data (e.g. response times, error logs, latency data)

For the avoidance of doubt:

- raw traffic recordings are not persistently stored
- only data necessary to create and execute test sequences is retained

leapwork

3.4 Additional Data for AI Studio
Where the Data Controller uses AI Studio, Customer Data may additionally include:

- AI interaction data, including prompts, assistant responses, and conversation history
- workflow state and generated outputs (e.g. test plans, code, and automation assets)
- uploaded files and knowledge-base data (e.g. documents, spreadsheets, PDFs, and extracted content)
- vector embeddings and structured data derived from uploaded materials
- remote browser session data, including visited URLs, rendered page content, screenshots, recorded actions, and execution context
- execution artifacts, including logs, run evidence, and reporting data

3.5 Special Categories of Personal Data
The Data Processor does not intentionally process special categories of personal data.

The Data Controller is responsible for ensuring that such data is not included in Customer Data unless appropriate safeguards are in place and permitted under applicable Data Protection Laws.

4. Purpose of Processing
The Data Processor processes personal data for the following purposes:

- provision, operation, and maintenance of the Offerings
- enabling the Data Controller to create, execute, and manage automated and performance testing workflows
- authentication, access control, and user management
- hosting and storage of Customer Data
- support, troubleshooting, and customer service
- analytics, reporting, and product improvement
- provision of AI-assisted features, where applicable

Where Leapwork Performance is used, additional purposes include:

- recording and transforming interaction data into test sequences
- simulating application and API behavior under load conditions
- executing performance testing workflows
- collecting and analysing performance metrics and execution data
- generating insights, including AI-assisted analysis of test results

Where AI Studio is used, additional purposes include:

- enabling AI-assisted test creation, planning, and automation
- processing and structuring user-provided content and documentation
- generating and maintaining test assets and automation workflows
- enabling remote browser automation and interaction recording
- storing and managing AI-assisted workflows, outputs, and associated data

5. Nature of Processing
Processing activities include:

- hosting and storage of data
- transmission, retrieval, and structuring of data

- execution of workflows defined by the Data Controller
- logging, monitoring, and diagnostics
- analysis of usage and system performance
- processing of data through AI-assisted features (where enabled)

Where Leapwork Performance is used, processing may additionally include:

- temporary storage of recording session data
- transformation of recorded interaction data into structured test sequences
- storage of test definitions, including request and response elements required for execution
- execution of performance tests across distributed infrastructure
- storage and analysis of test results, logs, and metrics

Where AI Studio is used, processing may additionally include:

- storage and management of AI interactions, including prompts, outputs, and workflow data
- ingestion and processing of customer-provided documents and knowledge-base materials
- generation and storage of code and automation artifacts
- execution of browser-based automation in remote environments
- capture and storage of execution artifacts, including screenshots and logs

For the avoidance of doubt, Leapwork strongly encourages Data Controller to only use de-identifiable and sanitized test data with the Offerings.

6. Duration
Personal data is processed for the duration of the Agreement and until the Data Controller either:

a) requests that the personal data be deleted; or
b) requests that the personal data be returned, with any copies being deleted by the Data Processor, except where retention is required under applicable law or for the establishment, exercise, or defence of legal claims.

Depending on the nature of the Offerings and the Data Controller's use thereof, certain categories of data may be subject to automated retention or deletion processes in accordance with the Data Processor's operational policies and the Data Controller's configuration of the Offerings.

Where AI-powered features are used, personal data may be processed by third-party AI providers for purposes such as inference, embedding generation, or related functionality. Such providers may retain data for limited periods in accordance with their operational and legal requirements.

In addition, certain AI-related data, including prompts, outputs, conversation history, and workflow data, may be stored by the Data Processor to support ongoing workflows, user functionality, and the management of automation assets within the Offerings.

For processing by (sub-) processors, any sub-processors, as listed in Annex 3, will be used solely to process the same subject matter and personal data as already processed by the Data Processor, and to the same nature and with the same duration as already described in this Annex 1.

7. General Conditions

- The Data Controller determines the content and use of Customer Data.

- The Data Processor processes personal data solely on documented instructions from the Data Controller.
- The Data Controller is responsible for ensuring that any personal data processed through the Offerings complies with applicable Data Protection Laws.
- The Data Processor recommends that the Data Controller use de-identified or sanitized test data where possible.

leapwork

ANNEX 2
Technical and Organisational Measures

1. Storage limitation

1.1 The Data Processor is required to limit the storage of personal data processed for the Data Controller by:

- Upon request from the Data Controller delete personal data concerning users.

2. Information security policy

2.1 The Data Processor shall have a documented information security policy, which is defined and approved by the management, published and communicated to its staff and other relevant parties.

3. Information security organisation

3.1 The Data Processor shall have staff with appointed responsibilities for ensuring an appropriate information security.

4. Staff security

4.1 The Data Processor shall in the recruitment process conduct adequate controls for applicants according to applicable legislations and ethic codes, which shall be in proportion to the business operations, the categories of personal data given access to and risk levels.

4.2 The Data Processor shall ensure that all personnel with access to personal data processed for the Data Controller have a confidentiality obligation towards the Data Processor and receive continued information security training.

4.3 The Data Processor shall have an employee offboarding process which includes removal of access rights and return of IT equipment.

5. Personal data handling

5.1 The Data Processor shall handle personal data processed for the Data Controller as confidential information.

6. Access Control

6.1 Users shall only have access to personal data, personal data processing resources, networks and network services that are needed to perform their duties and for which they have received explicit permission to access.

6.2 The Data Processor shall prevent unauthorised access to personal data processed for the Data Controller by (at least) implementing activity logs which register user activities and can give information about what personal data has been exposed to unauthorised access, modification, erasure or destruction.

leapwork

7. Physical security

7.1 Physical access to the Data Processor's systems and processing environment shall be restricted to authorised personnel.

7.2 Physical access to personal data processed for the Data Controller shall be restricted and require indentifiable and personal authentication scheme.

7.3 Equipment shall be placed and protected to minimise risks for environment related threats and dangers and unauthorised access.

8. Communication security

8.1 Personal data processing resources containing personal data or which are part of the system of the processing shall be protected by adequate security.

8.2 The Data Processor shall apply up-to-date security measures for electronic messages to actively protect against viruses, malware, ransonware and other harmfull software.

8.3 Development, test and production environments shall be separated to minimise the risk for unauthorised access or changes in the production and other environments.

8.4 Data from the Data Controller cannot be used in test or development environments without removing or anonymising personal data.

9. Confidentiality and non-disclosure agreements

9.1 The Data Processor shall ensure that requirements for confidentiality or non-disclosure agreements reflecting the Data Processor needs for the protection of information are identified, regularly reviewed and documented.

10. Information security awareness, education and training

10.1 The Data Processor shall ensure all of its employees and, where relevant, contractors, receive appropriate awareness education and training and regular updates in organizational policies and procedures. as relevant for their position.

11. Acceptable use of assets

11.1 The Data Processor shall implement rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.

12. Information systems audit controls

12.1 The Data Processor shall implement carefully planned and agreed upon audit requirements and activities involving verification of operational systems to minimize disruptions to business processes.

leapwork

13. Networks controls

13.1 The Data Processor shall ensure networks are managed and controlled to protect information in systems and applications snd ensure groups of information services, users and information systems are appropriately segregated.

14. Securing application services on public networks

14.1 The Data Processor shall ensure information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

15. System security and acceptance testing

15.1 The Data Processor shall ensure testing of security functionality is carried out during development and that acceptance testing programs and related criteria are established for new information systems, upgrades and new versions. The The Data Processor shall ensure test data is selected carefully, protected and controlled.

16. Electronic messaging

16.1 The Data Processor shall ensure information involved in electronic messaging shall be appropriately protected.

17. Controls against malware

17.1 The Data Processor shall implement detection prevention and recovery controls to protect against malware, combined with appropriate user awareness.

18. Management of technical vulnerabilities

18.1 The Data Processor shall implement technical vulnerabilities mitigation to reduce exposure to such vulnerabilities and ensure appropriate measures are taken to address the associated risk.

19. Planning information security continuity

19.1 The Data Processor shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or a disaster.

20. Information backup

20.1 The Data Processor shall implement a backup policy defining the requirements for backup of information, software and systems.

21. Access control policy

21.1 The Data Processor shall have an access control policy which is documented and reviewed periodically based on business and information security requirements.

leapwork

22. Policy on the use of cryptographic controls

22.1 The Data Processor shall have developed and implemented a policy on the use of cryptographic controls for the protection of the information.

23. Physical security perimeter

23.1 The Data Processor shall ensure that security perimeters are defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

24. Physical entry controls

24.1 The Data Processor shall ensure that secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

25. Secure disposal or re-use of equipment

25.1 The Data Processor shall ensure all equipment items containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

26. Media Disposal

26.1 The Data Processor shall ensure all media is disposed of securely when no longer required, using formal procedures.

27. Reporting and responding to information security events

27.1 The Data Processor shall ensure information security events are reported through appropriate management channels as quickly as possible and shall ensure information security incidents are responded to in accordance with the documented procedures.

leapwork

ANNEX 3
List of Sub-processors

The subprocessors listed below support the provision of Leapwork's Offerings. The specific subprocessors used in connection with a Customer's use of the Offerings may vary depending on the features, workflows, and configuration selected by the Customer. In particular, certain AI-related subprocessors are only engaged when customers actively use AI-assisted functionality.

Service	Service Provider / Sub-processor	Address	Hosting Location	Purpose
Microsoft Azure	Microsoft Corporation	United States	EU / global (including Netherlands)	Cloud infrastructure, hosting, storage, and data services
ChatGPT Enterprise Services	OpenAI, LLC	United States	United States	AI-powered data processing and analysis
Cloudmersive APIs	Cloudmersive, LLC	United States	United States	Data processing and API integration services
Retool	Retool, Inc.	United States	United States	Internal tools and data management
Auth0	Auth0, Inc. (Okta group)	United States	United States / EU	Authentication and identity management
LicenseSpring	LicenseSpring	Canada	Canada / United States	License management and enforcement
Microsoft Clarity	Microsoft Corporation	United States	Global	Product analytics and session insights
WorkOS	WorkOS, Inc.	Identity integration and authentication workflows	United States	Identity integration and authentication workflows
Claude Model Services	Anthropic PBC	United States	United States	AI-powered data processing and model inference
Gemini Model Services	Google LLC	United States	Global	AI-powered data processing and model inference

leapwork

Appendix A

EU Standard Contractual Clauses for the transfer of personal data to third countries

Where the transfer involves a transfer of EEA Protected Data outside of the EEA ("Ex-EEA Transfer") and the mechanisms referenced in Clause 7.2 (i) or (ii) of this DPA do not apply, such transfer shall be governed by the EU SCCs.

1. Controller-Processor

Considering that the processing activities between the Parties constitute a Controller-Processor relationship, Module 2 of the EU SCCs shall apply and shall be completed as follows:

i. All explanatory notes and footnotes deleted.

ii. As the Ex-EEA Transfer is a controller to processor transfer, only the provisions relating to Module 2 apply to such ex-EEA Transfer, and the provisions relating only to Modules 1, 3 and 4 are deleted and shall not apply to such ex-EEA Transfer.

iii. Clause 7 the Optional provision shall not apply.

iv. In respect of Clause 9 (sub-processors), Option 2 general written authorisation applies, and the minimum time period for the data importer to specifically inform the data exporter in writing of any intended changes to that list in accordance with Clause 9 shall be 7 days.

v. The "OPTION" in Clause 11(a) shall not apply and the wording in square brackets in that Clause shall be deleted.

vi. In respect of Clause 13(a) (supervision), the following wording shall apply: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I C, shall act as competent supervisory authority.

vii. In respect of Clause 17 (governing law), Option 1 shall apply, and the Member State governing law shall be the law of Denmark.

viii. In respect of Clause 18 (choice of forum and jurisdiction), the relevant courts shall be the courts of Denmark.

2. Appendix to the EU SCCs

In all cases, the Appendix to the EU SCCs shall be completed as follows:

- Annex I (A) is completed as follows in accordance with the data flows between the Parties:

  Data Exporter – where Data Controller is the exporter, this shall be completed with the Data Controller details as set out in this DPA; where Data Processor is the exporter, this shall be the Data Processor entity as defined in this DPA.

Data Importer – where Data Controller is the importer, this shall be completed with the Data Controller details as set out in this DPA; where Data Processor is the importer, this shall be the Data Processor entity as defined in this DPA.

- Annex I (B) is completed with the information set out in Annex 1 of this DPA.

- Annex I (C) is the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the EU SCCs in relation to the offering of goods or services to them.

- Annex II is completed with the information set out at Annex 2 of this DPA.

- Annex III is completed with the information set out at Annex 3 of this DPA.

3. Swiss Addendum to the EU SCCs

The Parties agree that for transfers of personal data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the terms of the EU SCCs shall be amended and supplemented as specified by the relevant guidance of the Swiss Federal Data Protection and Information Commissioner, and the following provisions shall apply:

i. General and specific references in the EU SCCs to GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

ii. In respect of data transfers governed by Swiss Data Protection Laws, the EU SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as personal data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

iii. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

iv. In respect of disputes, the choice of forum and jurisdiction as set out in the EU SCCs shall apply. For data subjects habitually resident in Switzerland, the law and courts of Switzerland are an alternative place of jurisdiction.

leapwork

Appendix B

UK STANDARD CONTRACTUAL CLAUSES

The Parties agree that to the extent there are transfers of Personal Data from the United Kingdom, and the mechanisms referenced in Clause 7.2 (i) or (ii) of this DPA do not apply, the UK SCCs shall apply and shall be incorporated hereby by reference.

In addition, where the UK SCCs identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

Part 1 - Tables:

- **Table 1:** For the purposes of Table 1 of the UK SCCs, the names of the parties, their roles and their details shall be set out as per the details stated in this DPA and the Agreement.
- **Table 2:** For the purposes of Table 2 of the UK SCCs, the boxes shall be completed with the information Appendix A which sets out the version of the EU SCCs which this UK SCCs are appended to, including the selected modules, clauses, optional provisions and Appendix Information. For the avoidance of doubt, England and Wales laws shall apply and English courts shall have jurisdiction.
- **Table 3:** "Appendix Information" is completed as set out in Annexes 1-3 of this DPA.
- **Table 4:** For the purposes of Table 4, the parties agree that neither the Importer nor the Exporter may end the UK Addendum as set out in Section 19.

Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, are incorporated by reference.

leapwork

Appendix C

CCPA ADDENDUM

This CCPA Addendum complements the DPA between Data Processor and Data Controller, and shall apply only to the extent Data Processor processes personal information of Californian residents that Data Controller provides or makes available to Data Processor in connection with the Agreement.

1. **Definitions**

i. The terms "***consumer***", "***device***", "***personal information***", "***processing***", "***sell***", "***service provider***" and "***third party***" shall have the meaning ascribed to them in the CCPA. For the avoidance of doubt, 'personal information' includes, but is not limited to, the types of data described in Annex A to the DPA. Capitalized terms not defined in this Addendum shall have the meanings set forth in the Agreement.

ii. "***Permitted Service Provider***" means third party service providers engaged by Data Processor to process Data Controller Personal Information on Data Processor's behalf to assist in the performance of the Offerings that are set out in Annex 3 to the DPA.

iii. "***Personal Information***" means all personal information of California residents that Data Controller provides or makes available to Data Processor, or that Data Processor otherwise processes on Data Controller's behalf, in each case, in connection with Data Processor's provision of the Offerings pursuant to the Agreement.

2. Processing of Personal Information

i. This Addendum applies to the collection, retention, use, disclosure, and sale of Personal Information.

ii. Data Controller is a business and appoints Data Processor as a service provider to process the Personal Information on behalf of Data Controller.

iii. Data Processor's collection, retention, use, disclosure, or sale of Personal Information for its own purposes independent of Data Controller 's use of the Offerings specified in the Agreement are outside the scope of this Addendum.

iv. Data Processor will comply with the CCPA and treat all Personal Data subject to the CCPA in accordance with the provisions of the CCPA. Data Processor will not:

(a) sell Personal Information;
(b) retain, use or disclose any Personal Information for any purpose other than for the specific purpose of providing the Offerings, including retaining, using or disclosing Personal Information for a commercial purpose other than providing the Offerings; or
(c) retain, use or disclose Personal Information outside of the direct business relationship between Data Processor and Data Controller.

v. The parties acknowledge and agree that the Processing of Personal Information authorized by Data Controller's instructions described in the Agreement and the DPA is integral to and encompassed by Data Processor's provision of the Offerings and the direct business relationship between the parties. The parties acknowledge and agree that Data Processor access to Data Controller's Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

vi. To the extent that any usage data is considered Personal Information, Data Processor is the business with respect to such data and will Process such data in accordance with its privacy policy found at https://www.leapwork.com/privacy-policy.

vii. Data Processor and Data Controller certify that they understand and will comply with the obligations and restrictions set forth in the DPA and the Agreement as required under the CCPA.