REMAPPED

Data Sub-Processing Addendum

1. INCORPORATION AND ACCEPTANCE

This Data Sub-Processing Addendum (the “Addendum”) forms part of the Applicable Terms referenced in the Partner Onboarding Agreement and/or related onboarding documentation (the “POP”).

By executing or otherwise accepting the POP, or by accessing or using the Services, the Partner agrees to be bound by this Addendum in its capacity as a sub-processor.

This Addendum applies without the need for separate execution.

2. PURPOSE AND CONTEXT

2.1 This Addendum governs the Processing of Personal Data by the Remapped (“Sub-Processor”) on behalf of Partner (“Processor”) in connection with the Services.

The Parties acknowledge that the Partner acts as processor on behalf of its clients, and Remapped processes Personal Data solely on behalf of and under the documented instructions of the Partner.

The Parties further acknowledge that, depending on the specific service configuration, Remapped may act as a processor in its own right (including, for example, where it processes Personal Data relating to Partner personnel or users of the platform), in which case the Partner shall act as controller.

Each Party shall comply with its obligations under Applicable Law in the role it performs in the relevant processing activity.

2.2 Use of Derived and Non-Personal Data

Nothing in this Addendum shall restrict Remapped’s use of data that has been aggregated, anonymized, de-identified, or otherwise derived from Personal Data, provided that such data does not identify any individual.

For the avoidance of doubt, this Addendum applies only to the Processing of Personal Data and does not limit Remapped’s ability to use such derived or non-personal data for service improvement, analytics, or the development of its technologies.

3. DEFINITIONS

For the purposes of this Addendum:

"**Applicable Law**" means all applicable laws relating to data protection and privacy, including the GDPR, UK GDPR, Data Protection Act 2018, e-Privacy Directive, and related implementing laws.

"**Data Security Measures**" means technical and organisational measures ensuring appropriate protection of Personal Data.

"**Instructions**" means this Addendum and any documented instructions provided by Partner acting as Processor, as derived from the applicable controller instructions.

"**Request**" means any governmental, regulatory, or law enforcement request for access to Personal Data.

"**Standard Contractual Clauses**" means Module 3 (Processor-to-Processor) of EU Decision 2021/914 and the UK Addendum.

"**Additional Sub-Processor**" means any third party engaged by Sub-Processor to process Personal Data.

All other capitalized terms shall have the meaning given under Applicable Law.

4. ROLES OF THE PARTIES

The Parties acknowledge that:

(a) The Partner acts as a processor on behalf of its clients;
(b) Remapped acts as a sub-processor of the Partner in connection with the provision of the Services; and
(c) Remapped shall process Personal Data solely on behalf of and under the Instructions of the Partner.

The Sub-Processor shall not determine the purposes or means of Processing.

The Parties further acknowledge that, in certain processing activities, Remapped may act as a processor in its own right, in which case the Partner shall act as controller and the Parties shall comply with their respective obligations under Applicable Law.

5. PROCESSING OBLIGATIONS

The Sub-Processor shall:

(a) process Personal Data only in accordance with Instructions;
(b) inform Partner if any Instruction infringes Applicable Law;
(c) ensure strict "need-to-know" access controls;
(d) ensure personnel are trained and bound by confidentiality obligations; and
(e) comply with Applicable Law.

6. DATA SUBJECT RIGHTS

The Sub-Processor shall:

(a) promptly notify Partner of any Data Subject request;
(b) not respond unless instructed; and
(c) assist Partner in complying with its legal obligations.

7. DATA SECURITY

The Sub-Processor shall implement and maintain appropriate Data Security Measures, including:

- encryption in transit and at rest;
- access controls and authentication;
- logging and monitoring;
- logical separation of data;
- secure data transmission;
- backup and availability controls.

Such measures shall be consistent with Annex 2.

8. INTERNATIONAL DATA TRANSFERS

The Sub-Processor shall not transfer Personal Data outside the EEA, UK or any jurisdiction not providing an adequate level of protection, unless:

(a) authorised by Partner;
(b) appropriate safeguards are implemented; and
(c) transfers comply with Applicable Law.

Where required:

- the Standard Contractual Clauses apply;
- Partner acts as data exporter;
- Sub-Processor acts as data importer.

The SCCs shall be deemed incorporated and completed by reference to this Addendum and its Annexes.

9. GOVERNMENT ACCESS AND SCHREMS II SAFEGUARDS

The Sub-Processor shall implement and maintain procedures to handle Requests and shall:

(a) notify Partner promptly where legally permitted;
(b) assess legality and challenge unlawful or disproportionate Requests;
(c) disclose only the minimum necessary Personal Data;
(d) remove identifying elements where possible;
(e) cooperate with Partner to contest or limit Requests;
(f) ensure Personal Data remains protected by confidentiality and security measures; and
(g) not disclose encryption keys or otherwise weaken security protections.

The Sub-Processor shall maintain records of Requests and provide aggregated information to Partner where legally permitted.

10. ADDITIONAL SAFEGUARDS

The Sub-Processor shall:

(a) ensure Personal Data is encrypted in transit;
(b) minimize the amount of Personal Data processed;
(c) apply pseudonymization where feasible;
(d) ensure data processing remains compliant with Applicable Law; and
(e) suspend processing where compliance cannot be ensured.

Partner may terminate processing where compliance cannot be restored within a reasonable period.

11. SUB-PROCESSING

The Sub-Processor shall not appoint Additional Sub-Processors without prior written authorization from Partner.

Where authorized:

(a) equivalent data protection obligations must be imposed;
(b) the Sub-Processor remains fully liable; and
(c) Partner shall be notified in advance of any changes, with a reasonable objection period.

12. DATA BREACH

The Sub-Processor shall:

(a) notify Partner without undue delay and within twenty-four (24) hours of becoming aware of a Personal Data Breach;
(b) provide all relevant information, including nature, impact, and mitigation measures; and
(c) cooperate fully in remediation and compliance efforts.

13. RETURN OR DELETION OF DATA

Upon termination or upon request, the Sub-Processor shall:

(a) return Personal Data; or
(b) securely delete or render it unreadable,

unless retention is required by Applicable Law.

14. AUDIT

The Sub-Processor shall:

(a) make available all information necessary to demonstrate compliance; and
(b) allow audits or inspections by Partner or its appointed auditor.

15. LIABILITY AND INDEMNITY

The Sub-Processor shall be liable for any breach of this Addendum and shall indemnify and hold harmless Partner against all losses, damages, costs, or claims arising from:

(a) breach of this Addendum;
(b) non-compliance with Applicable Law; or
(c) unauthorized or unlawful Processing.

16. ORDER OF PRECEDENCE

In the event of any conflict between this Addendum and other Applicable Terms, this Addendum shall prevail with respect to Personal Data processing.

17. ANNEXES

The following Annexes form part of this Addendum:
Annex 1: Description of Processing
Annex 2: Technical and Organisational Measures

18. GENERAL

This Addendum shall be governed by the governing law specified in the Applicable Terms.

This Addendum shall remain in effect for as long as Personal Data is processed by the Sub-Processor on behalf of Partner.

ANNEX 1

SCOPE OF THE DATA PROCESSING

This Annex forms part of the Data Processing Addendum between Partner and Sub-Processor (Remapped Ltd).
The nature of the Services is primarily focused on the analysis of technical, system, and infrastructure data. As such, the Services are designed to operate without requiring Personal Data, or with only very limited Personal Data strictly incidental to system operation.
In the unlikely event that Personal Data is processed, such data shall be limited to what is strictly necessary for the purposes described in this Annex and may include:

Categories of Data Subjects:

- Employees, contractors, and representatives of Partners's clients
- Employees, contractors, and representatives of the Partner and its affiliates
- IT users and system users whose data is included in infrastructure, application, or licensing environments
- Partners client personnel involved in IT, procurement, finance, or licensing functions

Categories of Personal Data:

- Identification data (e.g., name, username, user ID)
- Contact data (e.g., business email, business phone number)
- Professional data (e.g., job title, department, role)
- System and application usage data
- Device, infrastructure, and configuration data
- Licensing, entitlement, and deployment-related data
- Log data, access records, and system-generated identifiers

Personal Data processed is generally limited to business-related and technical data and does not typically include personal or private content.

Sensitive Data:

Processing of sensitive data is not intended.

The Sub-Processor shall not knowingly process special categories of Personal Data unless:

(a) expressly authorised in writing by Partner; and
(b) appropriate safeguards have been implemented in accordance with Applicable Law.

Nature and Purpose of Processing

The Processing is carried out for the following purposes:

- enabling access to and use of the Remapped platform;
- performing technical analysis of IT environments;
- supporting cloud optimization and licensing assessment (including OLA activities);
- collecting, structuring, and analysing system and configuration data;
- generating reports, insights, and evaluation outputs;
- supporting onboarding, evaluation, and related technical assistance activities;
- maintaining, operating, and improving the Service;
- ensuring system security, monitoring, and performance.

Processing is limited to what is necessary to support evaluation and onboarding activities.

Additional Sub-Processors

The Sub-Processor may engage Additional Sub-Processors in accordance with the Addendum.

- Such Additional Sub-Processors may include:
- cloud infrastructure providers
- hosting and data storage providers
- security and monitoring service providers
- technical support and maintenance providers

A current list of Additional Sub-Processors shall be made available by the Sub-Processor upon request or via the Applicable Terms.

Duration of Processing

Processing shall take place for the duration of:

- the applicable evaluation or onboarding period; and
- any additional period required for the provision of Services under the Applicable Terms.

Following termination, Personal Data shall be returned or deleted in accordance with the Addendum, unless retention is required by Applicable Law.

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES

Security Measures	
1.1.	**Access control to premises and facilities (physical)**: The following technical and organisational measures are in place to control access to premises and facilities. ● Access control system, card reader (e.g., magnetic card), numeric code ● Management of keys or documentation of key holders ● Door protection (e.g., electronic door openers) ● Security service, front desk ● Burglar alarm system ● CCTV
1.2.	**Access control to systems (virtual)**: The following technical and organisational measures are in place for user identification and authentication. ● Encryption of data in transit and at rest ● Personal and individual user log-in when entering the system and / or the corporate network ● Additional system log-in for special applications ● Automatic blocking of computer after a certain period of time without user activity (also password-protected screensavers or automatic pause function) ● User access logs
1.3.	**Access control to data**: The following measures are in place to ensure that data is accessed only by authorised employees in accordance with their access rights: ● Role-Based Access Control ● Authorisation routines ● Reports / data logs ● Reviews / Audits ● Restricted use of removable media (e.g. external hard drives), encryption and authorization prior to use
1.4.	**Disclosure control**: The following measures are in place to ensure secure transport, transmit, communicate or store data on data media (manual or electronic). ● Encryption of authorized removable media (e.g. external hard drive) ● Secure data networks (e.g., VPN)

	● Logging ● Remote access (e.g. client file transfers, web access) via dedicated endpoints in outer network.
1.5.	**Input control**: The following measures are in place for verifying and tracking whether data have been entered, changed, removed or deleted, and by whom. ● Access rights ● System logs ● Security/logging software ● Functional responsibilities
1.6.	**Availability control**: The following measures are in place to assure data availability and protect against accidental destruction or loss of data. ● Back-up processes ● Retention of back-ups ● Virus protection /firewall ● Hosting service provider in compliance with ISO 27001, 27017, 27018, in addition to SOC 1, 2, and 3
1.7.	**Separation control**: The following measures are in place to ensure that data processed for different purposes are processed separately. ● Encryption of client data in transit; encryption of all PII at field level within databases ● Separation of test, development and production environments