UBISECURE IDAAS DATA PROCESSING AGREEMENT

This Data Processing Agreement is made on __.__.20__ (“Effective Date”)

PARTIES AND PURPOSE

This Data Processing Agreement (“**DPA**”) is attached to and supplements Master Agreement ("Agreement") signed ____.____.20__ between _____ (“**Data Controller”**) (“**Customer**”, “**you**” or “**your**”) and Ubisecure Oy (“**Data Processor”), (“we”, “us”** or **"our"**).

The purpose of this DPA is to set out the terms and conditions for the processing of Personal Data by the Data Processor on behalf of the Data Controller, in accordance with the requirements of the applicable EU Data Protection Laws.

DEFINITIONS

The following definitions apply solely to this Data Processing Agreement:

“Master Agreement” means the document that includes this Data Processing Agreement as an appendix.

“Your Controlled Data” means Personal Data that Ubisecure processes on your behalf and according to your instructions as part of the Services, but only to the extent that you are subject to EU Data Protection Law in respect of such Personal Data.

“Applicable Protection Law” means any data protection or data privacy law or regulation of Switzerland, United Kingdom or any European Economic Area (“EEA”) country applicable to Your Controlled Data, including, as applicable, the EU General Data Protection Regulation 2016/679 and the e-Privacy Directive 2002/58/EC.

“GDPR” means the EU General Data Protection Regulation 2016/679.

The terms **“Data Controller”**, **“Data Processor”, “Data Subject”**, and **“Personal Data”** have the meanings given to these terms in the GDPR or secondarily in the EU Data Protection Law.

APPLICABILITY

This Data Processing Agreement only applies in respect of Your Controlled Data when your Data Subjects are residents within the EEA, UK or Switzerland.

CONFLICT RESOLUTION

In case of any conflict between the terms of the Master Agreement and the terms of this DPA, the relevant terms of this DPA shall take precedence, unless expressly stated otherwise.

PROCESSING ROLES AND ACTIVITIES

Ubisecure is the Data Processor for Your Controlled Data. Ubisecure will not access, use, or disclose Your Controlled Data to any third party except as provided in the Agreement, as necessary to maintain or provide the Services, or as necessary to comply with the law or binding order of a governmental, law enforcement or regulatory body. Ubisecure provides adequate data protection training to the employees and ensures that everyone authorized to process Your Controlled Data is competent and under a confidentiality obligation.

The Data Controller is responsible for ensuring that their instructions comply with all laws, regulations and rules applicable in relation to Your Controlled Data and that Your Controlled Data is collected lawfully by you or on your behalf and provided to us in accordance with such laws, rules and regulations. The Data Controller will also ensure that the processing of Your Controlled Data in accordance with your instructions will not cause us or you to breach any laws, rules or regulations (including the EU Data Protection Law).

OUR PROCESSING RESPONSIBILITIES AS THE DATA PROCESSOR

Notification of data breach. We will provide you notice without undue delay after becoming aware of and confirming the occurrence of any data breach, for which notification to you is required under the applicable EU Data Protection Laws. We will take appropriate measures to address the breach, including measures to mitigate any adverse effects resulting from the breach. We will, to assist you in complying with your notification obligations under Articles 33 and 34 of the GDPR, provide you with such information about the breach as we are reasonably able to disclose to you, considering the nature of the Services, the information available to us, and any restrictions on disclosing the information such as confidentiality.

Notification of Inquiry or Complaint. We will provide you notice, if permitted by applicable law, upon receiving an inquiry or complaint from a Data Subject, or other individual whose Personal Data is included in your content, or a binding demand (such as a court order or subpoena) from a government, law enforcement, regulatory or other body in respect of Your Controlled Data that we process on your behalf and instructions.

Reasonable Assistance with Compliance. We will, to the extent that you cannot reasonably do so through the Services, your account or otherwise, provide reasonable assistance to you in respect of your fulfilment of your obligation as the Data Controller to respond to requests by Data Subjects under Chapter 3 of the GDPR, considering the nature of the Services and information available to us. You will be responsible for our reasonable costs arising from our provision of such assistance.

Sub-Processors. You agree that we can share Your Controlled Data with the Sub-Processors listed in Annex 1 to provide you the Services. We will always make a written agreement with each Sub-Processor, ensure that the Sub-Processors are properly experienced and qualified, regularly monitor the performance of the Sub-Processors, and upon the Data Controllers request, provide the Data Controller with a list of all current Sub-Processors and processing locations of Personal Data, as well as information on the substance of the contract related to the data protection and security obligations within the Ubisecure - Sub-Processor relationship and the requirements of Article 30 of the GDPR. The current Sub-Processors are listed in Annex 1.

Data security. We have implemented and will maintain all times the technical and organizational measures to protect Personal Data against unlawful or unauthorized processing, access, copying, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, damage, alteration, or disclosure. These measures include but are not limited to: data encryption, physical and system level access control, threat and vulnerability management, security patch management, penetration testing, security training, security reviews and audits.

Ubisecure Certifications and Audits. Ubisecure performs security audits at least annually to verify the adequacy of our Security Measures. In addition to the information contained in this DPA,

upon Customer's request, We will make available the certificate issued for the ISO 27001 certification. Such audits will be performed by independent third-party security professionals at Ubisecure's selection and expense.

Destruction of Personal Data. Upon the termination of the Master Agreement or at the Data Controller's choosing, we shall at our own cost delete all Personal Data unless applicable law requires it to be stored. We may use our default Service Retention Periods for certain data types before deleting all data completely.

RIGHTS AND RESPONSIBILITIES OF THE DATA CONTROLLER

The Data Controller shall

process the Personal Data in compliance with the Data Protection Laws and good data processing practice;

give documented and binding instructions to the Data Processor on the processing of Personal Data;

at all times retain the control and authority to the Personal Data; and

at all times retain title and intellectual property rights and other rights to Personal Data.

maintain accurate contact information (email address) for Data Processor for important communications, such as Data Subject requests and data breach notifications

DATA TRANSFERS

You authorise us to transfer Your Controlled Data away from the country in which such data was originally collected. In particular, you authorise us to transfer Your Controlled Data to Finland and to all Sub-Processors specified in Annex 1, if any. We will not process Your Controlled Data without your prior written consent.

CATEGORIES OF PERSONAL DATA

The categories of Personal Data processed by the Data Processor and any Sub-Processor(s) are set out in Annex 1. The Data Processor and any Sub-Processor(s) may process such Personal Data only as long as the services are provided under the Agreement, and as long as one or more Parties have a right or obligation to process such data.

LIABILITY AND INDEMNIFICATION

The Parties agree that any Data Subject who has suffered damage as a result of any breach of this DPA is entitled to seek compensation primarily from the Party who has breached this DPA. If the other Party has paid damages to any Data Subject that are partly or fully attributable to the other Party, the former is entitled to claim back the relevant part of the damages from the latter.

Notwithstanding any limitations of liability, the parties agree that the Data Processor shall only be liable for any direct damages up to one million Euro, resulting from the Data Processor's breach of this DPA.

NOTICES

Notices regarding any dispute, claim or controversy arising out of or relating to this DPA and its annexes, or the breach, termination or validity thereof shall be deemed sufficient if made in writing and delivered by registered mail, by courier or by email to the recipient at the address specified below or at other address that the receiving Party has supplied in writing. Each Party is entitled to change their contact persons by informing in writing the other Party thereof. Also notices regarding any Personal Data Breaches and changes in data processing shall be made to the following Customer contact:

If to the Customer: _____

If to the Data Processor: support(a)ubisecure.com

TERM AND TERMINATION

This DPA shall automatically terminate upon any termination or expiration of the Master Agreement, AND all the Personal Data is, at the Data Controller's choosing, either deleted or returned to the Data Controller, unless Law requires it to be stored in part or in whole. If separate assignments for processing of Personal Data independent of the Agreement have been concluded by and between the Parties in accordance with the form in Annex 1, this DPA shall automatically terminate when the Agreement and all such separate assignments have terminated or expired. The Data Processor shall certify that the actions have taken place and, upon request, provide the Data Controller with technical evidence of permanent destruction of all Personal Data.

The terms and conditions of this DPA which are meant to survive the termination or expiry of this DPA shall survive such termination or expiry and be binding between the Parties. In particular, termination or expiration of this DPA shall not discharge the Processor from its confidentiality obligations and the Processor agrees to, even after the termination or expiry of this DPA, to perform all its legal obligations as the Processor and to assist the Controller in its performance of its legal obligations pursuant to the Data Protection Laws. To the extent that the Personal Data is processed by the Processor, for whatsoever reason, after the termination or expiration of the Agreement, this DPA shall continue to apply to such processing for as long as such processing is carried out, unless agreed otherwise.

APPLICABLE LAW AND SEVERABILITY

This DPA shall in all respects be governed by and interpreted in accordance with the laws of Finland apart from its conflict of laws provisions. If any provision of this DPA shall be invalid, unenforceable or ineffective for any reason whatsoever, all other provisions hereof shall be and remain in full force and effect.

SIGNATURES

AS WITNESS this DPA has been duly executed by the Parties on the date stated at the beginning of this DPA.

Data Processor		**Data Controller**	
Ubisecure Oy			_____
By:	_____	By:	_____
Print Name:	_____	Print name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

ANNEX 1

Personal Data Processing categories, purposes, and Sub-Processors.

CATEGORIES OF PROCESSING

- Ubisecure IDaaS (Identity and Access Management Service)
- Ubisecure IDaaS Product Support Services

CATEGORIES OF DATA SUBJECTS

The Data Processor processes Personal Data on the following categories of Data Subjects (please select only the options relevant to the processing carried out under the DPA):

- ☐ Employees, including job applicants and agency contract workers
- ☐ Customers and customer employees
- ☐ Potential customers and employees of potential customers
- ☐ Partners, such as suppliers and their employees
- ☐ Other, please specify:

_____

TYPES OF PERSONAL DATA

The Data Processor processes Personal Data on the following categories of Data Subjects (please select only the options relevant to the processing carried out under the DPA):

- ☐ *Name and other identification information* such as first name, last name, home address, email address, telephone number, and/or mobile number
- ☐ *Individualisation data* such as date of birth, nationality, sex, and/or age
- ☐ *Employment and human resources data* such as title, employment history, employee assessments, disciplinary actions, communications, salary, bank account number and/or training data
- ☐ *National identification number or equivalent government-issued unique identifier*
- ☐ *Technical or security data* such as IP addresses, other technical identifiers, metadata, and/or data on technical or security events such as access control log data or system monitoring data
- ☐ *Special categories of personal data* such as trade union membership, health data, biometrics, political opinions, racial or ethnic origin and/or criminal convictions
- ☐ *Other*, please specify:

_____

SUB-PROCESSORS

Supplier	Role	Data Processed	Location
Amazon Web Services (AWS)	Primary hosting provider for Ubisecure IDaaS (test and production environments)	Customer personal data (PII) and other operational data stored in Identity Cloud	EU
Atlassian (Service Management)	Handling customer technical support requests via Ubisecure Support Service Desk	Customer personal data (PII) provided in support tickets	Australia
BetterStack (Betterstack.com)	Centralized log management and alerting platform	Log data including technical and security event information and customer personal data (PII)	USA

SUB-PROCESSORS OF AMAZON WEB SERVICES

Amazon Web Services states that a current list of its sub-processors is freely available at:
https://aws.amazon.com/compliance/sub-processors/
Ubisecure will provide a list of Amazon Web Services' current Sub-Processors on request. Ubisecure will also notify the Data Controller at least 14 days before any changes to this list take effect, and will forward any objection to processing without undue delay.

SUB-PROCESSORS OF ATLASSIAN

Atlassian states that a current list of its sub-processors is freely available at:
https://www.atlassian.com/legal/sub-processors
Ubisecure will provide a list of Atlassian's current Sub-Processors on request. Ubisecure will also notify the Data Controller at least 14 days before any changes to this list take effect, and will forward any objection to processing without undue delay.

SUB-PROCESSORS OF BETTERSTACK

BetterStack states that a current list of its sub-processors is freely available at:
https://betterstack.com/dpa/schedules
Ubisecure will provide a list of BetterStack's current Sub-Processors on request. Ubisecure will also notify the Data Controller at least 14 days before any changes to this list take effect, and will forward any objection to processing without undue delay.

ANNEX 2 – DATA TRANSFERS FROM THE EUROPEAN ECONOMIC AREA

The Standard Contractual Clauses are an integral part of this agreement.
Ubisecure shall ensure that any Restricted Transfer by Ubisecure to an approved Sub-Processor is subject to the applicable module of the Standard Contractual Clauses or another valid transfer mechanism as defined in Articles 45 and 46 of the GDPR.

Where Personal Data protected by the EU Data Protection Law is transferred, either directly or via onward transfer, to a country outside of EU that is not subject to an adequacy decision, the following applies:

(a) The EU SCCs are hereby incorporated into this DPA by reference as follows:

(i) Ubisecure is the "data exporter" and the Data Processor / Sub-Processor is the "data importer."
(ii) Module Two (Controller to Processor) applies where Ubisecure is a Controller of Personal Data
(iii) Module Three (Processor to Processor) applies where Ubisecure is a Data Processor of Personal Data
(iv) By entering into this DPA, each party is deemed to have signed the EU SCCs, as included in the European Commission implementing decision (EU) 2021/914 dated June 4th 2021, as of the commencement date of the Agreement.

(b) For each Module, where applicable:

(i) In Clause 7, the optional docking clause applies with the exception of Atlassian Pty Ltd, Australia.
(ii) In Clause 9, Option 2 applies, and the time period for prior notice of a Sub-processor change is 14 days.
(iii) In Clause 11, the optional language does not apply.
(iv) In Clause 17, Option 1 applies, and the EU SCCs are governed by Finnish law.
(v) In Clause 18(b), disputes will be resolved before the courts of Finland.
(vi) The Appendix of EU SCCs is populated as follows:

The information required for Annex I(A) is located in the Master Agreement and/or relevant Orders.
The information required for Annex I(B) is located in Annex 1 of this DPA.
The competent supervisory authority in Annex I(C) will be determined in accordance with the Applicable Data Protection Law in Finland.
The information required for Annex II is located in Ubisecure's Information Security Management System (ISMS) and Transfer Impact Assessment, summary of which is made available for Controllers at no cost, and the Data Processing Agreements of the individual Sub-processors.
The information required for Annex III is location in Annex 1 of this DPA.

ANNEX 3 – DATA TRANSFERS FROM THE UNITED KINGDOM

In case of any transfers of Personal Data from the United Kingdom, the following provisions apply: This annex provides the addendum that has been issued by the Information Commissioner for parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Where this annex uses capitalized terms that are defined in the DPA, including the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. Other capitalized terms have the meanings provided by the Addendum B.1.0, issued by the Information Commissioner's Office and laid before the United Kingdom Parliament in accordance with section 119A of the Data Protection Act 2018 on February 2, 2022.

Part 1: Tables

Table 1: Parties

As pursuant under section "PARTIES AND PURPOSE" and Annex 1.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: As pursuant to the effective date of the DPA. Reference (if any): Commission Implementing Decision (EU) 2021/914 of 4 June 2021. Other identifier (if any): Not applicable. Or ☐ The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As pursuant under section "PARTIES AND PURPOSE" and Annex 1.
Annex 1B: Description of Transfer: The categories of Personal Data processed are set out in Annex 1.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Ubisecure maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in its Information Security Management System and Data Protection Impact Assessment. Ubisecure regularly reviews compliance with these safeguards and will not materially decrease the overall security of the Service during a subscription term. Ubisecure conducts reasonable due diligence and security assessments of its Sub-processors, and enters into agreements with Sub-processors that contain provisions similar to or more stringent than those provided for in this DPA. As necessary, Ubisecure will work directly with Sub-processors to provide assistance to the Data Controller.
Annex III: List of Sub processors (Modules 2 and 3 only): The list of Sub-Processors is in Annex 1.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before the United Kingdom Parliament in accordance with section 119A of the Data Protection Act 2018 on February 2, 2022, as it is revised under section 18 of those Mandatory Clauses.

ANNEX 4 – DATA TRANSFERS FROM SWITZERLAND

In case of any transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the Standard Contractual Clauses apply with the following modifications:

1. General and specific references in the Standard Contractual Clauses to GDPR, EU, EEA or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws, as applicable.

2. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, 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.

3. For Data Subjects resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.