DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends and forms part of the written agreement between Customer and Oden Technologies Ltd. ("**Vendor**") (the "**Agreement**"). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

1. **Definitions**

1.1. **In this DPA:**

a) "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in Data Protection Law;

b) "**Customer Personal Data**" means any Customer Data that constitutes Personal Data, the Processing of which is subject to Data Protection Law, for which Customer or Customer's customers are the Controller, and which is Processed by Vendor to provide the Services, as defined in the Agreement;

c) "**Data Protection Law**" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and the e-Privacy Directive 2002/58/EC, and all other data protection laws of the European Union, the European Economic Area ("**EEA**"), including the European Union, and all other data protection laws of the EEA, the UK General Data Protection Regulation and the UK Data Protection Act 2018, each as applicable, and as may be amended or replaced from time to time;

d) "**Data Subject Rights**" means all rights granted to Data Subjects by Data Protection Law, including the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;

e) "**International Data Transfer**" means any transfer of Customer Personal Data from the EEA, or the United Kingdom to a country outside of the EEA and the United Kingdom, and includes any onward transfer of Customer Personal Data from the country outside of the EEA, or the United Kingdom to another international organization or to another country outside of the EEA, and the United Kingdom;

f) "**Personnel**" means any natural person acting under the authority of Vendor;

g) "**Sensitive Data**" means any type of Customer Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under Data Protection Law or other laws to which the Controller is subject;

h) "**Subprocessor**" means a Processor engaged by a Processor to carry out Processing on behalf of a Controller;

i) "**Standard Contractual Clauses**" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended from time to time;

j) "**Third-Party Controller**" means a Controller for which Customer is a Processor; and

k) "**UK Addendum**" means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

2. **Scope and applicability**

2.1. This DPA applies to Processing of Customer Personal Data by Vendor to provide the Services.

2.2. The subject matter, nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Annex I**, which is an integral part of this DPA.

2.3.   Customer is a Controller and appoints Vendor as a Processor on behalf of Customer. Customer is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

2.4.   To the extent that Customer is a Processor on behalf of a Third-Party Controller, Customer engages Vendor as a Processor to Process Customer Personal Data on behalf of that Third-Party Controller. To the extent necessary for Customer or a Third-Party Controller to comply with Data Protection Law, Customer may assign certain or all rights granted to Customer in this DPA to that Third-Party Controller. In such case, Customer is the single point of contact for Vendor; must obtain all necessary authorizations from such Third-Party Controller(s); undertakes to issue all instructions and exercise all rights on behalf of such other Controller(s); and is responsible for compliance with the requirements of Data Protection Law applicable to Processors.

2.5.   Customer acknowledges that Vendor may Process Customer Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, product development, and compliance with law. Vendor is the Controller for such Processing and will Process such data in accordance with Data Protection Law.

3.   Instructions

3.1.   Vendor will only Process Customer Personal Data to provide the Services and on documented instructions of Customer or a Third-Party Controller.

3.2.   Customer and Third-Party Controller's instructions are documented in **Annex I**, the Agreement, and any applicable statement of work.

3.3.   Both Customer and Third-Party Controller may issue additional instructions to Vendor as necessary to comply with Data Protection Law.

3.4.   Unless prohibited by applicable law, Vendor will inform Customer if Vendor is subject to a legal obligation that requires Vendor to Process Customer Personal Data in contravention of Customer's documented instructions.

4.   Subprocessing

4.1.   Customer hereby authorizes Vendor to engage Subprocessors. A list of Vendor's current Subprocessors is listed in **Annex III**.

4.2.   Vendor will inform Customer prior to any intended change of Subprocessor. Customer may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Vendor's notification of the intended change. Customer and Vendor will work together in good faith to address Customer's objection. If Vendor chooses to retain the Subprocessor, Vendor will inform Customer at least thirty (30) days before authorizing the Subprocessor to Process Customer Personal Data, and Customer may immediately discontinue using the relevant parts of the Services, and may terminate the relevant parts of the Services within thirty (30) days.

4.3.   Vendor must enter into a written agreement with all Subprocessors which imposes the same obligations on the Subprocessors as this DPA imposes on Vendor.

5.   International Data Transfers

5.1.   Vendor must obtain Customer's specific prior written authorization to perform International Data Transfers. Customer hereby authorizes Vendor to transfer Customer Personal Data subject to Data Protection Law to any country deemed adequate by the EU Commission, or for transfers from the UK deemed adequate by the UK Government; on the basis of appropriate safeguards in accordance with Data Protection Law; or pursuant to the Standard Contractual Clauses. By signing this DPA, Customer and Vendor conclude Module 2 (controller-to-processor) of the Standard Contractual Clauses, which are hereby incorporated and completed as follows: the "data

exporter" is Customer; the "data importer" is Vendor; the optional docking clause in Clause 7 is implemented; Clause 9(a) option 2 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is struck; Clause 17 option 1 is implemented and the governing law is Ireland; the courts in Clause 18(b) are Dublin, Ireland; Annex 1, 2 and 3 to module 2 of the Standard Contractual Clauses are Annex I, II and III to this DPA respectively.

5.2.   By signing this DPA, Customer and Vendor conclude the UK Addendum, which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Vendor, their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in **Section 5.1** of this DPA; (iii) in Table 3, Annexes 1 (A and B) to the "Approved EU SCCs" are Annex I, II, and III to this DPA respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum

Vendor must inform Customer at least thirty (30) days prior to any intended change of International Data Transfers, including the country, and the legal basis of the International Data Transfer pursuant to Section 5.1.

5.3.   If either party's compliance with Data Protection Law applicable to International Data Transfers is affected by circumstances outside of either party's control, including if a legal instrument for transfers is invalidated, amended, or replaced, then the parties will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative standard contractual clauses are approved by the relevant data protection authorities, the Vendor reserves the right to amend the Agreement and this DPA by adding to, changing or replacing, the standard contractual clauses that form part of it at the date of signature in order to ensure continued compliance with Data Protection Law.

6.   Personnel

6.1.   Vendor must ensure that all Personnel authorized to Process Customer Personal Data are subject to a contractual or statutory obligation of confidentiality.

7.   Security and Personal Data Breaches

7.1.   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 for the rights and freedoms of natural persons, Vendor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in **Annex II**.

7.2.   Customer acknowledges that the security measures in **Annex II** are appropriate in relation to the risks associated with Customer's intended Processing and will notify Vendor prior to any intended Processing for which Vendor's security measures may not be appropriate.

7.3.   Vendor must inform Customer without undue delay after becoming aware of a Personal Data Breach. If Vendor's notice or subsequent notices are delayed, they must be accompanied by reasons for the delay.

8.   Assistance

8.1.   Taking into account the nature of the Processing, and the information available to Vendor, Vendor will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfillment of Customer's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct Data Protection Impact Assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

8.2.   Vendor will maintain records of Processing of Customer Personal Data in accordance with Data Protection Law.

8.3.   Vendor may charge a reasonable fee for assistance under this **Section 8**. If Vendor is at fault, Customer and Vendor shall each bear their own costs related to assistance.

9. Audit

9.1. Upon reasonable request, Vendor must make available to Customer all information necessary to demonstrate compliance with the obligations of Data Protection Law and this DPA and allow for and contribute to audits, including inspections, conducted by a Supervisory Authority, Customer or another auditor mandated by Customer, as mandated by a Supervisory Authority or as reasonably requested no more than once per year by Customer. The foregoing shall only extend to those documents and facilities relevant and material to the Processing of Customer Personal Data and shall be conducted during normal business hours and in a manner that causes minimal disruption.

9.2. Vendor will inform Customer if Vendor believes that Customer's instruction under **Section 9.1** infringes Data Protection Law. Vendor may suspend the audit or inspection or withhold requested information until Customer has modified or confirmed the lawfulness of the instructions in writing.

9.3. Customer and Vendor each bear their own costs related to an audit.

10. Liability

10.1. Where Vendor has paid compensation, damages or fines, Vendor is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer's part of responsibility for the compensation, damages or fines.

11. Notifications

11.1. Vendor must make all notifications required under this DPA at least to Peter Brand, President and COO via email to peter.brand@oden.io and legal@oden.io.

11.2. Vendor must make all notifications relating to the security of Processing to the contact identified in Section 11.1 and to Deepak Turaga via email Deepak.turaga@oden.io.

12. Term and duration of Processing

12.1. The Processing will last no longer than the term of the Agreement.

12.2. Upon termination of the Processing, Vendor must, at Customer's choice, delete or return all Customer Personal Data and must delete all remaining copies within ninety (90) days after confirmation of Customer's choice. Unless required or permitted by applicable law, Vendor will delete all remaining copies of Customer Personal Data within one hundred eighty (180) days after returning Customer Personal Data to Customer.

12.3. This DPA is terminated upon Vendor's deletion of all remaining copies of Customer Personal Data in accordance with Section 12.2.

13. Modification of this DPA

13.1. This DPA may only be modified by a written amendment signed by both Customer and Vendor.

14. Invalidity and severability

14.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

ODEN TECHNOLOGIES
Make things. Better.

ANNEX I

A. LIST OF PARTIES

Customer is the data exporter and Vendor is the data importer.

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

#	Category	Description
1	Users of platform	Users who have been granted an email login to the Oden platform.

2. Categories of personal data transferred:

#	Category	Description
1	Email address	Used to identify and manage users, deliver transactional report and alert emails, measure product usage by login, and log errors in web platform
2	IP address	Used to measure product usage, log errors in web platform
3	Location	City/region/country, used to measure product usage, inferred from IP address
4	Job Title	Used to analyze product usage by job role
5	Phone Numbers	For Multi-factor authentication, we also use phone numbers that are made available to a third party (Okta)

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N./A.

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Customer Personal Data is transferred on a continuous basis.

5. Nature of the processing

Customer Personal Data is transferred for the provision of the Services.

6. Purpose(s) of the data transfer and further processing:

#	Operation	Description
1	User management	Viewing, adding, and modifying user logins within an account.
2	Email delivery	Sending transactional emails to subscribed users within an account.
3	Error logging	Logging of errors produced within Oden web services which may include user email and IP address.
4	Product usage tracking	Measurement of feature usage within Oden web platform, associated with user's email address.
5	Location determination	Identification of user's city inferred from IP address, for product usage analytics.
6	Multi-factor authentication	Phone numbers are used a secondary mechanism while logging into the Oden platform.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Customer Personal Data will be retained in accordance with applicable statute of limitations and applicable laws, including Data Protection Law.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

For the nature and subject matter and nature, we refer to the Agreement and the DPA. The duration of the processing will be the duration of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority will be designated in accordance with the DPA.

ANNEX II

SECURITY MEASURES

Vendor and Data Importer will, at a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Personal Data are Processed, include:

    [X]   Access control system (ID reader, magnetic card, chip card);

    [X]   Key management, card-keys procedures;

    [X]   Door locking (electric door openers etc.);

    [X]   Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

    [X]   User identification and authentication procedures;

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Personal Data in accordance with their access rights, and that Customer Personal Data cannot be read, copied, modified or deleted without authorization, include:

    [X]   Internal policies and procedures;

    [X]   Control authorization schemes;

    [X]   Differentiated access rights (profiles, roles, transactions and objects);

    [X]   Monitoring and logging of accesses; and

    [X]   Change procedure;

4. Disclosure control

Technical and organizational measures to ensure that Customer Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

    [X]   Transport security.

5. Control of instructions

Technical and organizational measures to ensure that Customer Personal Data are Processed solely in accordance with the

instructions of the Controller include:

[X]   Unambiguous wording of the contract.

6. Availability control

Technical and organizational measures to ensure that Customer Personal Data are protected against accidental destruction or loss (physical/logical) include:

[X]   Backup procedures;

[X]   Mirroring of hard disks (e.g. RAID technology);

[X]   Uninterruptible power supply (UPS);

[X]   Remote storage;

[X]   Anti-virus/firewall systems; and

[X]   Disaster recovery plan.

7. Separation control

Technical and organizational measures to ensure that Customer Personal Data collected for different purposes can be Processed separately include:

[X]   Segregation of functions (production/testing); and

[X]   Procedures for storage, amendment, deletion, transmission of data for different purposes.

ANNEX III

SUBPROCESSORS

Customer authorizes Vendor to engage the following Subprocessors:

#	Name	Address	Contact details	Description
1	Google Ireland Limited	Gordon House, Barrow Street, Dublin, D04 E5W5, Dublin, Ireland		Cloud data storage and processing
	Mixpanel,	405 Howard Street, Floor 2, San Francisco, CA, 94105		Product usage analytics
	SendGrid,	1801 California Street, Suite 500, Denver, CO, 80202		Delivery of transactional emails to users
	Functional Software, Inc dba "Sentry"	132 Hawthorne Street, San Francisco, CA, 94107		Monitoring of errors in web platform
	Hound Technology, Inc. d/b/a Honeycomb	548 Market St, San Francisco CA 94104		Application performance monitoring

	Okta, Inc.	100 First St, 6th Floor, San Francisco CA 94105		User authentication services
	LaunchDarkly	1999 Harrison St Suite 1100, Oakland, CA 94612		To selectively release new features to customers