

[ LEGAL AGREEMENT ]

# Data Processing Agreement

Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)

This Data Processing Agreement (the "Agreement" or "DPA") forms part of, and is subject to, the agreement between the Controller and Owl Owl OÜ (the "Processor") for the provision of the Services. It governs the processing of personal data carried out by the Processor on behalf of the Controller.

THE PROCESSOR	THE CONTROLLER
Owl Owl OÜ Sepapaja tn 6 15551 Tallinn, Estonia hi@o.ee	Name _____ Address _____ _____ Email _____

Effective date \_\_\_\_\_

Together the "Parties", each individually a "Party".

## [1] Definitions

Capitalised terms have the meaning given to them in the GDPR. In particular: "GDPR" means Regulation (EU) 2016/679; "personal data", "processing", "controller", "processor", "data subject", "sub-processor" and "supervisory authority" have the meanings set out in Article 4 GDPR. "Services" means the services provided by the Processor to the Controller.

## [2] Subject Matter and Roles

1. The Controller determines the purposes and means of processing and acts as the data controller. The Processor processes personal data on behalf of the Controller and acts as the data processor.
2. The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.
3. This Agreement applies for as long as the Processor processes personal data on behalf of the Controller in connection with the Services.

## [3] Processing on Documented Instructions

1. The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers to a third country, unless required to do so by Union or Member State law; in such a case the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.
2. The Controller's complete and final instructions at the time of signing are set out in this Agreement and the underlying service agreement. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions.

## [4] Confidentiality

The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that access is limited to personnel who need it to provide the Services.

## [5] Security of Processing

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 to the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.
2. The technical and organisational measures are described in Annex 2. The Processor may update these measures provided the level of security is not materially reduced.

## [6] Sub-Processors

1. The Controller grants the Processor a general authorisation to engage sub-processors. A current list is set out in Annex 3.
2. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object to such changes.

3. The Processor shall impose on each sub-processor, by contract, the same data protection obligations as set out in this Agreement, and remains fully liable to the Controller for the performance of that sub-processor's obligations.

### **[7] Assistance to the Controller**

1. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests to exercise the data subject's rights under Chapter III GDPR.
2. The Processor shall assist the Controller in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor – including security, breach notification, data protection impact assessments and prior consultation.

### **[8] Personal Data Breaches**

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach affecting the Controller's personal data, and shall provide sufficient information to allow the Controller to meet its obligations under Articles 33 and 34 GDPR.

### **[9] International Transfers**

Personal data is processed within the European Union / European Economic Area. The Processor shall not transfer personal data to a third country or international organisation outside the EEA unless an adequacy decision applies or appropriate safeguards under Article 46 GDPR (such as the European Commission's Standard Contractual Clauses) are in place.

### **[10] Deletion or Return of Data**

At the choice of the Controller, the Processor shall delete or return all personal data after the end of the provision of the Services, and delete existing copies unless Union or Member State law requires storage. Where the Controller uses self-service deletion features, deleting an account removes the associated personal data from active systems, subject to short technical backup retention cycles.

### **[11] Audits and Inspections**

The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Audits shall take place on reasonable prior notice, during business hours, and in a manner that does not disproportionately disrupt the Processor's operations.

### **[12] Liability, Term and Governing Law**

1. Each Party's liability arising out of or related to this Agreement is subject to the limitations and exclusions of liability in the underlying service agreement.
2. This Agreement takes effect on the effective date and remains in force for the duration of the processing of personal data by the Processor on behalf of the Controller.
3. This Agreement is governed by the laws of Estonia and the European Union. In the event of a conflict with the underlying service agreement, this Agreement prevails with respect to the processing of personal data.

### [13] Signatures

FOR THE PROCESSOR

Owl Owl OÜ

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date \_\_\_\_\_

FOR THE CONTROLLER

\_\_\_\_\_

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date \_\_\_\_\_

ANNEX 1

## Details of the Processing

---

<b>Subject matter</b>	Provision of the Services described in the underlying service agreement (operation of the federated and hosting platforms run by Owl Owl OÜ, including C.IM, P.LU, R.NF and Image.Hosting).
<b>Duration</b>	For the term of the service agreement and until deletion or return of the personal data under Clause 10.
<b>Nature &amp; purpose</b>	Hosting, storage, transmission, display and moderation of user accounts and user-generated content in order to deliver the Services.
<b>Data subjects</b>	End users and account holders authorised by the Controller; individuals whose personal data appears in content they submit.
<b>Personal data</b>	Account identifiers (username, email address), profile information, user-generated content, and technical data such as IP addresses and access logs.
<b>Special categories</b>	Not intended. The Controller shall not instruct the processing of special categories of data (Article 9 GDPR) unless expressly agreed in writing.

ANNEX 2

## Technical and Organisational Measures

---

The Processor maintains measures appropriate to the risk, including without limitation:

- [+] **Encryption in transit** – HTTPS/TLS is enforced across all public services.
- [+] **Access control** – administrative access is restricted to authorised personnel on a need-to-know basis and protected by strong authentication.
- [+] **Hosting location** – infrastructure and data are located within the EU / EEA.
- [+] **Confidentiality** – personnel with access are bound by confidentiality obligations.
- [+] **Resilience** – regular backups and measures to restore availability after an incident.
- [+] **Logging & monitoring** – access and security logs are retained for abuse prevention and reviewed where appropriate.
- [+] **Data minimisation** – only the personal data necessary to operate the Services is collected, with no advertising or behavioural profiling.
- [+] **Incident response** – procedures to detect, assess and report personal data breaches.

ANNEX 3

## Sub-Processors

---

The Processor engages the following categories of sub-processors to deliver the Services. The current list is available on request from hi@o.ee.

Sub-processor / category	Purpose	Location
--------------------------	---------	----------

---

Infrastructure & hosting	Server, storage and network infrastructure	EU / EEA
CDN / DDoS protection	Delivery, caching and security of web traffic	EU / Global*
Payment processors	Processing of voluntary donations	EU / Global*

---

\* Where a sub-processor processes personal data outside the EEA, appropriate safeguards under Article 46 GDPR apply.

---

This is a template Data Processing Agreement provided by Owl Owl OÜ for convenience and does not constitute legal advice. Owl Owl OÜ · Sepapaja tn 6, 15551 Tallinn, Estonia · hi@o.ee