

Data Processing Agreement

pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) — between the licence holder (the “Controller”) and Eco Heroes International SL (the “Processor”)

Controller: _____ (name of the school, school group, hotel or company as stated in the licence agreement), represented by _____.

Processor: Eco Heroes International SL, Spain, represented by Karim Zouhdi, founder. Contact for data protection matters: info@eco-heroes.org.

This Agreement forms part of, and is governed by, the Eco Heroes licence agreement (the “Licence”). In case of conflict regarding the processing of personal data, this Agreement prevails.

1. Subject matter and duration

The Processor provides the Eco Heroes platform (the SDG adventure game, trivia, student and teacher handbooks, missions, progress tracking and optional LMS integration) under the Licence. The Processor processes personal data on behalf of the Controller for the duration of the Licence and until deletion or return under clause 9.

2. Nature and purpose of the processing; categories

The nature, purpose, categories of data subjects and categories of personal data are set out in **Annex I**. The Processor shall process personal data only for the purposes described there.

3. Obligations of the Processor

The Processor shall:

1. 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 informs the Controller of that legal requirement before processing, unless the law prohibits it on important grounds of public interest;
2. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. implement the technical and organisational measures set out in **Annex II** and maintain a level of security appropriate to the risk in accordance with Article 32 GDPR;
4. respect the conditions of clause 5 for engaging another processor;
5. taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests for exercising data-subject rights (Articles 12–23 GDPR), within 10 business days of a request;
6. assist the Controller in ensuring compliance with Articles 32–36 GDPR, taking into account the nature of the processing and the information available to the Processor;
7. at the choice of the Controller, delete or return all personal data after the end of the provision of services, and delete existing copies unless Union or Member State law requires storage (clause 9);

8. make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits (clause 8);
9. immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data-protection provisions.

4. Obligations of the Controller

The Controller is responsible for the lawfulness of the processing, for providing the information required by Articles 13 and 14 GDPR to data subjects (including parents and guardians where applicable), for obtaining any consents required under national law for pupils below the age of digital consent, and for the accuracy of the data it enters into the platform. The Controller shall issue instructions in writing (e-mail suffices).

5. Sub-processors

The Controller gives general authorisation to the engagement of the sub-processors listed in **Annex III**. The Processor shall inform the Controller of any intended addition or replacement of sub-processors at least **30 days** in advance by e-mail to the Controller's administrator contact and by updating <https://eco-heroes.org/trust/>, giving the Controller the opportunity to object on reasonable, data-protection-related grounds. If an objection cannot be resolved, the Controller may terminate the affected part of the Licence without penalty. The Processor imposes 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 sub-processor's performance.

6. International transfers

Personal data is hosted and processed in the European Union (Hetzner Online GmbH data centres in Germany and Finland). Where a sub-processor processes personal data outside the EU/EEA, the transfer is based on an adequacy decision (including the EU–US Data Privacy Framework for certified organisations) or on the Standard Contractual Clauses adopted by the European Commission (Decision (EU) 2021/914), supplemented where necessary.

7. Personal data breach

The Processor shall notify the Controller without undue delay, and in any case within **48 hours** of becoming aware of a personal data breach affecting the Controller's data, providing the information required by Article 33(3) GDPR insofar as available, and shall cooperate with the Controller in investigating, mitigating and documenting the breach.

8. Audit and information

The Processor shall, on request and at most once per contract year (or additionally following a personal data breach), provide the Controller with the information necessary to demonstrate compliance, including the current security overview and sub-processor list. Where this is insufficient, the Controller or an independent auditor bound by confidentiality may audit the Processor's relevant processing activities with at least 30 days' notice, during business hours and without unreasonable disruption. Each party bears its own costs.

9. Deletion and return

Upon termination of the Licence, the Processor shall, at the Controller's choice, return the Controller's personal data in a structured, commonly used format (CSV) and/or delete it. In the absence of an instruction, personal data is deleted **within 30 days of a written request** and in any event **no later than 24 months after the end of the**

Licence. Backups are overwritten in the ordinary backup cycle (at most 90 days). The Processor confirms deletion in writing on request.

10. Liability, term and governing law

Liability is governed by the Licence and Article 82 GDPR. This Agreement enters into force on the start date of the Licence and ends when all personal data has been deleted or returned. It is governed by the law of Spain and of the European Union; the parties submit to the courts competent for the Processor's registered office, without prejudice to mandatory consumer or public-procurement rules applicable to the Controller.

For the Controller	For the Processor — Eco Heroes International SL
Name, position, date, signature	Karim Zouhdi, founder — date, signature

Annex I — Details of the processing

Subject matter	Provision of the Eco Heroes learning platform to the Controller's students, teachers and administrators.
Nature	Hosting, storage, display, progress tracking, certificate generation, optional transmission of grades to the Controller's LMS (LTI), support.
Purpose	Delivery of sustainability education (UN Sustainable Development Goals) under the Licence; no other purpose.
Categories of data subjects	Students (typically aged 9–17); teachers; school administrators; guest participants (hotel and corporate licences).
Categories of personal data — students	First name or nickname; avatar; class code; language; progress and quiz results; XP and badges; time of activity. Not collected: e-mail, photograph, date of birth, address, location, device identifiers for advertising.
Categories of personal data — teachers / administrators	Name, work e-mail, school, role, language, hashed password, login times, classes created, support correspondence.
Special categories	None are requested or required. The Controller shall instruct users not to enter special-category data in free-text fields.
Retention	Duration of the Licence; deletion per clause 9.

Annex II — Technical and organisational measures

1. Transport encryption: TLS 1.2+ only, HTTP Strict Transport Security, automatic certificate renewal.
2. Content-Security-Policy with per-script hashes and nonces (no unsafe-inline), strict framing (frame-ancestors 'none'), no third-party scripts except consent-gated analytics.
3. Authentication: teacher passwords hashed with bcrypt (cost factor 12); access codes stored only as keyed HMAC hashes; e-mail verification before first login; session revocation on password change; rate limiting on login, registration and code redemption; constant-time comparisons; CSRF tokens on every form.
4. Tenant isolation: school administrators can only access users, codes and progress belonging to their own school; super-administrator access is restricted to the Processor's staff.
5. Data minimisation: no student e-mail addresses, photographs or dates of birth are collected; analytics only after explicit consent; third-party video embedded in privacy-enhanced mode and loaded only on user action.
6. Availability and recovery: backups before every release with a tested rollback procedure; the previous production version is retained; CDN-level DDoS and bot protection.
7. Logging and monitoring: security-relevant events (failed logins, code redemptions, CSP violation reports) are logged with hashed IP addresses; logs are retained for 90 days.
8. Organisational: access to production systems is limited to named persons with multi-factor authentication; changes are reviewed and tested before release; a vulnerability-disclosure channel is published at /.well-known/security.txt and reports are answered within 5 business days.

The current, more detailed security overview is published at <https://eco-heroes.org/trust/#security> and is reviewed with every release.

Annex III — Authorised sub-processors

Sub-processor	Purpose	Location	Transfer safeguard
Hetzner Online GmbH	Application hosting, database, backups	Germany / Finland (EU)	Art. 28 contract (Hetzner DPA)
Cloudflare, Inc.	CDN, TLS termination, DDoS and bot protection	Global edge; EU data regions	EU–US Data Privacy Framework; SCCs
Google Ireland Ltd (Analytics 4)	Aggregate usage statistics, only after the user's consent	EU/US	DPF; SCCs; IP anonymisation
Google Ireland Ltd (YouTube, youtube-nocookie.com)	Playback of curated educational videos, loaded only on user action	EU/US	DPF; privacy-enhanced mode
The Controller's own LMS (e.g. Moodle)	Optional LTI 1.1/1.3 integration configured and controlled by the Controller	Controller's choice	Controller's own contract

Stripe and Formspree process data for family subscriptions and the general contact form respectively; they do not process student data under school, hotel or corporate licences and are therefore not sub-processors under this Agreement.

Eco Heroes International SL · info@eco-heroes.org · <https://eco-heroes.org/trust/> · Data Processing Agreement v1.0, 9 October 2026. This document is published for evaluation; the signed version forms part of the Licence.