Questa è una traduzione fornita per comodità. La versione inglese è il testo giuridicamente vincolante e prevale in caso di qualsiasi divergenza. English (PDF)

Accordo sul trattamento dei dati

ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 (RGPD) e dell'articolo 33 della Legge organica spagnola 3/2018, del 5 dicembre, sulla protezione dei dati personali e la garanzia dei diritti digitali (LOPDGDD) — tra il licenziatario (il «Titolare») ed Eco Heroes International SL (il «Responsabile»)

Parti e ruoli

Titolare: _____ (nome della scuola, del gruppo di scuole, dell'autorità scolastica, dell'impresa o dell'hotel indicato nella Licenza), con sede in _____, rappresentato da _____ (nome, ruolo).
Referente del Titolare per la protezione dei dati (referente amministratore o, se nominato, responsabile della protezione dei dati): _____.

Responsabile: Eco Heroes International SL, CIF B44915940, con sede legale in 17003 Girona (Spagna), iscritta nel Registro Mercantil de Girona, rappresentata da Karim Zouhdi, fondatore. Referente per la protezione dei dati: info@eco-heroes.org, +34 690 814 215. Segnalazioni di sicurezza: security@eco-heroes.org (si veda https://eco-heroes.org/.well-known/security.txt).

Ruoli. Il Titolare decide perché e come sono trattati i Dati del Titolare ed è il titolare del trattamento di tali dati. Il Responsabile tratta i Dati del Titolare esclusivamente per conto del Titolare, in qualità di responsabile del trattamento ai sensi dell'articolo 4, punto 8, del RGPD.

Account insegnante. Ogni insegnante ha un account personale e nominativo. Il Responsabile gestisce l'account in sé (accesso, sicurezza, autenticazione a due fattori e risorse gratuite per insegnanti) in qualità di titolare del trattamento, secondo la propria Informativa sulla privacy. Tutto ciò che un insegnante fa nel Servizio per il Titolare costituisce Dati del Titolare: il ruolo e i diritti dell'account nell'organizzazione del Titolare, le classi, gli alunni, i progressi, i compiti, i quiz dal vivo, le importazioni di elenchi di classe, gli avvii dalla piattaforma di apprendimento e gli studi di impatto.

Fuori dal presente Accordo. L'Allegato I, sezione B, elenca i trattamenti di cui il Responsabile è esso stesso titolare. Tali trattamenti sono disciplinati dall'Informativa sulla privacy del Responsabile (https://eco-heroes.org/legal/privacy/) e non dal presente Accordo. Eco Heroes Academy (learn.eco-heroes.org) e la valutazione VSME (assessment.eco-heroes.org) sono servizi distinti, con propri termini e informative sulla privacy; il presente Accordo non li copre.

Il presente Accordo fa parte della Licenza. In caso di contrasto tra la Licenza e il presente Accordo in materia di trattamento dei dati personali, prevale il presente Accordo.

Definizioni

- **«Licenza»** indica il contratto in base al quale il Titolare utilizza il Servizio: il preventivo o l'ordine accettato dal Titolare, insieme alle Condizioni di licenza per scuole e organizzazioni pubblicate all'indirizzo https://eco-heroes.org/legal/licence/.
- **«Servizio»** indica la piattaforma Eco Heroes e l'assistenza descritte nella clausola 1.1.
- **«Dati del Titolare»** indica i dati personali che il Responsabile tratta per conto del Titolare ai sensi del presente Accordo, descritti nell'Allegato I, sezione A.
- **«Utenti»** indica gli alunni, gli insegnanti, gli amministratori scolastici, i dipendenti, il personale, gli ospiti e le altre persone che il Titolare autorizza a utilizzare il Servizio.
- **«Sub-responsabile»** indica un altro responsabile del trattamento di cui il Responsabile si avvale per trattare Dati del Titolare.
- **«Giorno lavorativo»** indica dal lunedì al venerdì, esclusi i giorni festivi a Girona (Spagna).
- I termini definiti nell'articolo 4 del RGPD, come «dati personali», «trattamento» e «violazione dei dati personali», hanno lo stesso significato nel presente Accordo.

1. Oggetto e durata

1.1 Il Responsabile fornisce il Servizio al Titolare ai sensi della Licenza. Il Servizio comprende: il gioco di avventura, il quiz, i giochi di parole e i quiz di classe dal vivo; i libri illustrati e la Story Library, i video delle missioni, i manuali e le schede didattiche; gli account insegnante nominativi, la gestione delle classi e i compiti; l'importazione facoltativa di elenchi di classe (CSV, CSV OneRoster, Google Classroom); l'accesso facoltativo degli insegnanti con Google o Microsoft; il collegamento facoltativo alla piattaforma di apprendimento del Titolare tramite LTI 1.1 o LTI 1.3; il pannello di classe dell'app mobile Eco Heroes, se il Titolare lo utilizza; gli studi di impatto facoltativi; per le licenze per imprese e hotel, account di coordinatore, gruppi con codici di accesso per i figli dei dipendenti o degli ospiti e rapporti sui progressi per gruppo (CSV), un report aggregato dell'organizzazione, certificati con il nome dell'organizzazione e l'accesso facoltativo del personale tramite il provider di identità del Titolare; e l'assistenza.

1.2 Il Responsabile tratta i Dati del Titolare per la durata della Licenza e fino a quando tutti i Dati del Titolare siano stati cancellati o restituiti ai sensi della clausola 10.

2. Natura e finalità del trattamento; categorie

2.1 L'**Allegato I** descrive la natura e la finalità del trattamento, le categorie di interessati e le categorie di dati personali.

2.2 Il Responsabile tratta i Dati del Titolare unicamente per fornire il Servizio al Titolare. Non li utilizza per pubblicità, per creare profili degli alunni che vadano oltre i progressi di apprendimento che il Servizio mostra agli insegnanti del Titolare, per vendere o noleggiare dati, né per sviluppare un prodotto diverso dal Servizio.

2.3 **Statistiche anonimizzate.** Quando il Titolare iscrive classi a uno studio di impatto, incarica il Responsabile di elaborare statistiche aggregate a partire dalle risposte, che il Responsabile può utilizzare nei propri rapporti e pubblicazioni. Il Responsabile aggrega solo risposte di gruppi di almeno 10 alunni, non vi include mai risposte a testo libero e verifica che nessun alunno, classe o scuola possa essere identificato. Le statistiche così ottenute non sono più dati personali. Il Titolare può revocare questa istruzione in qualsiasi momento con comunicazione scritta; le risposte raccolte successivamente sono utilizzate solo per i risultati propri del Titolare.

3. Istruzioni

3.1 Il Responsabile tratta i Dati del Titolare soltanto su istruzione documentata del Titolare, anche in caso di trasferimento verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o dello Stato membro cui il Responsabile è soggetto. In tal caso, il Responsabile informa il Titolare di tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

3.2 Costituiscono istruzioni documentate del Titolare il presente Accordo, la Licenza e le impostazioni che il Titolare e i suoi Utenti scelgono nel Servizio (per esempio creare classi, importare elenchi di classe, attivare l'accesso unico o un collegamento a una piattaforma di apprendimento, iscrivere una classe a uno studio di impatto, cancellare alunni o classi). Il referente amministratore del Titolare impartisce ogni ulteriore istruzione per iscritto; è sufficiente un'e-mail a info@eco-heroes.org.

3.3 Il Responsabile informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il RGPD, la LOPDGDD o altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Il Responsabile può sospendere l'esecuzione di tale istruzione finché il Titolare non la conferma o la modifica.

4. Obblighi del Titolare

4.1 Il Titolare è responsabile della liceità del trattamento, compresa la base giuridica per il trattamento dei dati degli alunni; della fornitura agli interessati delle informazioni previste dagli articoli 13 e 14 del RGPD (alunni e, se del caso, i loro genitori o tutori, insegnanti, amministratori, dipendenti e ospiti); dell'ottenimento di ogni consenso che la legge applicabile al Titolare richiede per gli alunni al di sotto dell'età del consenso digitale (articolo 8 del RGPD; articolo 7 della LOPDGDD: 14 anni in Spagna); e dell'esattezza dei dati che esso e i suoi Utenti inseriscono.

4.2 Il Titolare chiede ai propri Utenti di non inserire categorie particolari di dati personali (articolo 9 del RGPD), cognomi, indirizzi e-mail o altri identificativi diretti degli alunni nei campi a testo libero, come soprannomi, nomi delle classi, note dei compiti, soprannomi dei quiz dal vivo e risposte ai sondaggi.

4.3 Quando il Titolare collega la propria piattaforma di apprendimento (LTI) o il proprio fornitore di identità (accesso unico), è responsabile di tale sistema e della sua configurazione, affinché condivida soltanto i dati descritti nell'Allegato I (per gli alunni tramite LTI, solo il nome e mai l'indirizzo e-mail).

4.4 Il Titolare nomina un referente amministratore e, prima di svolgere uno studio di impatto, un referente per la tutela dei minori, e mantiene aggiornati entrambi i contatti nel Servizio o tramite e-mail al Responsabile. Finché non è nominato un referente per la tutela dei minori, o finché l'account del referente nominato è chiuso, il Servizio trasmette le segnalazioni di tutela dei minori agli amministratori scolastici del Titolare. Per le classi non collegate a una scuola nel Servizio (per esempio classi usate solo tramite un avvio LTI), le segnalazioni vanno al referente per la tutela dei minori del Responsabile, che le trasmette senza indugio al referente amministratore del Titolare.

5. Obblighi del Responsabile

Il Responsabile:

a. tratta i Dati del Titolare soltanto ai sensi della clausola 3;

b. garantisce che le persone autorizzate al trattamento dei Dati del Titolare si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, e che l'accesso ai sistemi di

produzione sia limitato a persone nominativamente individuate che ne hanno bisogno;

c. adotta le misure tecniche e organizzative dell'**Allegato II** e mantiene un livello di sicurezza adeguato al rischio ai sensi dell'articolo 32 del RGPD, tenuto conto che tra gli interessati vi sono minori;

d. ricorre a un altro responsabile del trattamento soltanto alle condizioni della clausola 6;

e. tenendo conto della natura del trattamento, assiste il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato (articoli da 12 a 23 del RGPD), come previsto dalla clausola 8;

f. assiste il Titolare nel garantire il rispetto degli articoli da 32 a 36 del RGPD (sicurezza, notifica delle violazioni, valutazione d'impatto sulla protezione dei dati, consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a sua disposizione; la sintesi della valutazione d'impatto vigente del Responsabile è pubblicata nel Trust Centre e la valutazione completa è messa a disposizione del Titolare su richiesta;

g. su scelta del Titolare, cancella o restituisce tutti i Dati del Titolare al termine del Servizio e cancella le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro ne preveda la conservazione (clausola 10);

h. mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dell'articolo 28 del RGPD e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un revisore da esso incaricato (clausola 11);

i. tiene un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare (articolo 30, paragrafo 2, del RGPD);

j. trasferisce Dati del Titolare verso un paese terzo soltanto alle condizioni della clausola 7.

6. Sub-responsabili

6.1 Il Titolare concede un'autorizzazione scritta generale per i Sub-responsabili elencati nell'**Allegato III, Parte A**.

6.2 Il Responsabile informa il Titolare di qualsiasi aggiunta o sostituzione prevista di un Sub-responsabile con almeno **30 giorni** di anticipo, tramite e-mail al referente amministratore del Titolare e aggiornando https://eco-heroes.org/trust/. Il Titolare può opporsi per motivi ragionevoli legati alla protezione dei dati. Se l'opposizione non può essere risolta entro il periodo di preavviso, il Titolare può recedere dalla parte interessata della Licenza senza penali, e si applica la clausola 10.

6.3 Il Responsabile si avvale di ciascun Sub-responsabile in base alle condizioni standard di trattamento dei dati di tale fornitore. Tali condizioni impongono al Sub-responsabile obblighi in materia di protezione dei dati che presentano garanzie sufficienti per l'adozione di misure tecniche e organizzative adeguate, come richiesto dall'articolo 28, paragrafo 4, del RGPD. Il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento di tali obblighi da parte di ciascun Sub-responsabile.

6.4 L'**Allegato III, Parte B** elenca i servizi di terzi che il Responsabile utilizza ma che **non trattano** Dati del Titolare. Essi non trattano dati personali, oppure trattano soltanto dati di cui il Responsabile è esso stesso titolare. Sono elencati per trasparenza e non sono Sub-responsabili ai sensi del presente Accordo.

6.5 I sistemi propri del Titolare, come la sua piattaforma di apprendimento o il suo ambiente Google o Microsoft, sono scelti e controllati dal Titolare. Non sono Sub-responsabili del Responsabile.

7. Trasferimenti internazionali

7.1 I Dati del Titolare sono ospitati e memorizzati nell'Unione europea: i server applicativi in Francia (Internet Girona, su infrastruttura OVHcloud); il database, i backup cifrati e un server di riserva in Germania e Finlandia (Hetzner Online GmbH). La rete di distribuzione dei contenuti (Cloudflare) serve pagine pubbliche memorizzate nella cache dalla sua rete globale. Le risposte contenenti dati personali sono contrassegnate come private e non memorizzabili (no-store), e la rete non le memorizza nella cache.

7.2 Il Responsabile non trasferisce Dati del Titolare al di fuori dello Spazio economico europeo, né consente a un Sub-responsabile di farlo, salvo che (i) la destinazione benefici di una decisione di adeguatezza della Commissione europea, compresa la Svizzera e, per le organizzazioni di cui il Responsabile ha verificato la certificazione nell'elenco ufficiale, il quadro UE-USA per la protezione dei dati personali; oppure (ii) sulla base delle clausole contrattuali tipo adottate con la decisione di esecuzione (UE) 2021/914 della Commissione (modulo 3, da responsabile a responsabile, o modulo 2 se del caso), integrate da misure supplementari qualora una valutazione del trasferimento ne dimostri la necessità. L'Allegato III indica la garanzia applicabile a ciascun Sub-responsabile. Il Responsabile conserva per iscritto una valutazione del trasferimento per ciascun Sub-responsabile al di fuori del SEE e la mette a disposizione del Titolare su richiesta.

7.3 Cloudflare, Inc. termina la connessione cifrata ai margini della propria rete e vi tratta pertanto dati di richiesta (indirizzo IP, indirizzo richiesto, intestazioni). Il Responsabile si basa sulle condizioni standard di trattamento dei dati di Cloudflare comprendenti le clausole contrattuali tipo e, se Cloudflare figura nell'elenco ufficiale del quadro per la protezione dei dati, sul quadro UE-USA per la protezione dei dati personali.

7.4 Proton AG ospita la posta elettronica del Responsabile in Svizzera. La Svizzera beneficia di una decisione di adeguatezza della Commissione europea.

8. Assistenza per i diritti degli interessati

8.1 Gli insegnanti possono visualizzare, esportare (CSV), rinominare, azzerare e cancellare i dati di un alunno, e cancellare intere classi, direttamente nel Servizio. Ogni insegnante vede soltanto le proprie classi; gli amministratori scolastici vedono tutte le classi della propria scuola e possono revocare immediatamente l'accesso di un insegnante. Il Titolare utilizza queste funzioni per rispondere alle richieste ogni volta che può.

8.2 Se una richiesta non può essere soddisfatta tramite il Servizio, il Responsabile assiste il Titolare entro **10 giorni lavorativi** da una richiesta scritta. Se il Responsabile riceve direttamente da un interessato (compreso un genitore o tutore) una richiesta relativa a Dati del Titolare, non risponde nel merito. Indirizza l'interessato al Titolare senza indebito ritardo e ne informa il Titolare, salvo diversa istruzione di quest'ultimo.

9. Violazione dei dati personali

9.1 Il Responsabile notifica al Titolare qualsiasi violazione dei dati personali che riguardi Dati del Titolare senza ingiustificato ritardo e comunque entro **48 ore** dal momento in cui ne è venuto a conoscenza. La prima notifica contiene le informazioni richieste dall'articolo 33, paragrafo 3, del RGPD nella misura in cui siano note in quel momento: la natura della violazione, le categorie e il numero approssimativo di interessati e di registrazioni coinvolti, le probabili conseguenze e le misure adottate o proposte. Il Responsabile integra tali informazioni in fasi successive man mano che diventano disponibili.

9.2 Il Responsabile collabora con il Titolare per indagare, contenere e documentare la violazione e lo assiste in qualsiasi notifica all'autorità di controllo (in Spagna, l'Agencia Española de Protección de Datos) e in qualsiasi comunicazione agli interessati. Il Responsabile documenta qualsiasi violazione dei dati personali, comprese le circostanze, le conseguenze e i provvedimenti adottati.

9.3 Il Responsabile invia le notifiche via e-mail al referente amministratore del Titolare. Chiunque può segnalare una vulnerabilità di sicurezza a security@eco-heroes.org. Le segnalazioni ricevono un avviso di ricevimento entro 5 giorni lavorativi e i problemi critici vengono risolti prima di qualsiasi altro lavoro.

10. Conservazione, cancellazione e restituzione

10.1 **Durante la Licenza.** I Dati del Titolare sono conservati secondo il calendario dell'Allegato I, sezione C, che rispecchia le regole di conservazione applicate nel codice del Servizio. Un insegnante può cancellare un alunno o una classe in qualsiasi momento, con effetto immediato nel database attivo e nella replica di riserva.

10.2 **Esportazione.** Durante la Licenza, e fino alla cancellazione prevista dalla clausola 10.3, il Titolare può esportare nel Servizio i dati di classe e dei progressi in formato CSV, oppure chiedere al Responsabile un'esportazione in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

10.3 **Fine della Licenza.** Se la Licenza termina e non viene rinnovata, il Responsabile cancella i Dati del Titolare **90 giorni** dopo la data di cessazione. Se il Titolare lo richiede per iscritto, il Responsabile cancella i Dati del Titolare entro **30 giorni** dalla richiesta, che la Licenza sia terminata o meno. Il Responsabile conferma la cancellazione per iscritto su richiesta. Prima della cancellazione, il Responsabile invia un'e-mail agli amministratori scolastici del Titolare 30 giorni e 7 giorni prima della data di cancellazione, indicando tale data e come rinnovare la Licenza o esportare i dati; la cancellazione non avviene prima che siano trascorsi 30 giorni dal primo messaggio e 7 giorni dal secondo.

10.4 **Account insegnante.** Quando l'ultima licenza collegata a un account insegnante termina, l'account prosegue come account insegnante gratuito. Viene cancellato 12 mesi dopo la fine di tale licenza, salvo che nel frattempo l'insegnante sia collegato a una nuova licenza; un account gratuito viene cancellato dopo 12 mesi senza accessi. Il Responsabile invia un'e-mail all'insegnante 30 giorni prima della cancellazione. Il mantenimento di un account insegnante non conserva alcun Dato del Titolare: tali dati sono cancellati ai sensi della clausola 10.3.

10.5 **Backup e replica.** I dati cancellati escono dai backup nel normale ciclo. I backup cifrati sono conservati a rotazione, cosicché i dati cancellati escono da tutti i backup entro **14 giorni**. La replica in sola lettura sul server di riserva recepisce ogni cancellazione in modo continuo. I backup sono ripristinati solo per rimediare a una perdita del sistema di produzione; se un ripristino reintroduce dati cancellati, la cancellazione viene applicata di nuovo.

10.6 **Conservazione per obbligo di legge.** Il Responsabile conserva dati personali dopo la fine della Licenza solo nella misura e per il tempo richiesti dal diritto dell'Unione o dello Stato membro, per esempio fatture e scritture contabili per 6 anni ai sensi dell'articolo 30 del Codice di commercio spagnolo (Código de Comercio). Tali documenti identificano le persone di contatto del Titolare e non contengono dati degli alunni. Il Responsabile li protegge secondo l'Allegato II e non li utilizza per altre finalità.

11. Revisione e informazioni

11.1 Su richiesta, e non più di una volta per anno contrattuale (o in aggiunta dopo una violazione dei dati personali o in caso di sospetto documentato e ragionevole di inosservanza), il Responsabile fornisce al Titolare le informazioni necessarie per dimostrare il rispetto del presente Accordo. Esse comprendono la sintesi di sicurezza vigente (https://eco-heroes.org/trust/#security), l'elenco vigente dei Sub-responsabili, il registro dei trattamenti svolti per conto del Titolare, le valutazioni dei trasferimenti, la valutazione d'impatto sulla protezione dei dati, gli ultimi risultati delle prove di ripristino e delle esercitazioni di commutazione e i risultati di eventuali revisioni di sicurezza.

11.2 Se tali informazioni non sono sufficienti, il Titolare, o un revisore indipendente da esso incaricato e vincolato alla riservatezza, può sottoporre a revisione i trattamenti pertinenti del Responsabile con un preavviso di almeno **30 giorni**, durante l'orario lavorativo e senza perturbare in modo irragionevole l'attività del Responsabile o di altri clienti. Ciascuna parte sostiene i propri costi. Il Responsabile può chiedere al revisore di sottoscrivere un ragionevole impegno di riservatezza e limitare l'accesso ai sistemi condivisi con altri clienti a quanto necessario per verificare la conformità.

12. Responsabilità

12.1 Ciascuna parte risponde nei confronti degli interessati ai sensi dell'articolo 82 del RGPD. Tra le parti, la responsabilità è disciplinata dalla clausola sulla responsabilità della Licenza. Nessuna disposizione del presente Accordo o della Licenza limita la responsabilità di una parte ove la legge non consenta di limitarla, compresa la responsabilità per dolo.

12.2 Se il Responsabile deve pagare una sanzione amministrativa o un risarcimento a causa delle istruzioni del Titolare o perché il Titolare non ha adempiuto ai propri obblighi ai sensi della clausola 4, il Titolare tiene indenne il Responsabile nella misura di tale causa, e viceversa.

13. Durata, legge applicabile e foro competente

13.1 Il presente Accordo entra in vigore alla data di inizio della Licenza e termina quando tutti i Dati del Titolare sono stati cancellati o restituiti ai sensi della clausola 10. Le clausole 5(b), 10, 11 e 12 continuano ad applicarsi per il tempo necessario.

13.2 Il presente Accordo è disciplinato dal diritto spagnolo e dal diritto dell'Unione europea, compresi il RGPD e la LOPDGDD. Sono competenti i tribunali di Girona (Spagna), fatte salve le norme imperative applicabili al Titolare in quanto ente pubblico o ai sensi della normativa sugli appalti pubblici, e fatti salvi i diritti degli interessati ai sensi dell'articolo 79 del RGPD. L'Allegato V aggiunge le regole per i titolari nel Regno Unito e negli Stati Uniti.

13.3 Qualsiasi modifica del presente Accordo deve essere fatta per iscritto; è sufficiente un'e-mail. Il Responsabile pubblica il modello vigente all'indirizzo https://eco-heroes.org/trust/. Una nuova versione del modello non modifica un Accordo firmato senza il consenso del Titolare. L'amministratore scolastico del Titolare può accettare il presente Accordo online; il Responsabile registra chi lo ha accettato, quando, quale versione e un hash con chiave dell'indirizzo IP utilizzato.

Firme

Per il Titolare	Per il Responsabile — Eco Heroes International SL
Nome, ruolo	Karim Zouhdi, fondatore
Data, firma	Data, firma

Allegato I — Descrizione del trattamento

A. Trattamento per conto del Titolare (oggetto del presente Accordo)

Allegato I.A — trattamento per conto del Titolare

Voce	Descrizione
Oggetto	Fornitura del Servizio agli Utenti del Titolare ai sensi della Licenza.
Natura	Hosting, memorizzazione, visualizzazione e cancellazione di dati; monitoraggio dei progressi; quiz di classe dal vivo; compiti; certificati; gestione delle classi; importazione facoltativa di elenchi di classe forniti dal Titolare (incolla o caricamento CSV, CSV OneRoster 1.1/1.2, Google Classroom); avvii facoltativi LTI 1.1 / LTI 1.3 dalla piattaforma di apprendimento del Titolare, con Names and Role Provisioning (importazione degli elenchi) e Assignment and Grade Services (restituzione dei punteggi); accesso facoltativo degli insegnanti con Google o Microsoft scelto dal Titolare; pannello di classe dell'app mobile Eco Heroes quando il Titolare distribuisce un codice classe; questionari facoltativi degli studi di impatto nelle classi iscritte dal Titolare; account di coordinatore, codici di accesso di gruppo e rapporti sui progressi per gruppo (CSV) per le licenze per imprese e hotel; assistenza. Per le licenze aziendali e per hotel, inoltre: report di attività aggregati per l'organizzazione (report dell'organizzazione e totali, con ogni dato basato su meno di 5 famiglie nascosto) e una classifica a squadre facoltativa; nome e logo dell'organizzazione sui certificati dei bambini; accesso facoltativo del personale tramite il provider di identità del Titolare stesso (OpenID Connect).
Finalità	Offrire un'educazione allo sviluppo sostenibile basata sugli Obiettivi di sviluppo sostenibile delle Nazioni Unite, con il monitoraggio dei progressi, la rendicontazione e la valutazione previsti dalla Licenza. Per gli studi di impatto: la valutazione del proprio insegnamento da parte del Titolare (risultati di classe per i suoi insegnanti) e statistiche aggregate e anonimizzate ai sensi della clausola 2.3. Nessun'altra finalità.
Categorie di interessati	Alunni (il gioco è pensato per i 9–17 anni in due fasce d'età, 9–12 e 13–17; le schede didattiche stampabili coprono le fasce 6–10, 11–13 e 14–17 anni, e il Titolare può utilizzare il Servizio con alunni più piccoli a propria discrezione); insegnanti; amministratori scolastici; genitori e tutori, solo quando si utilizza la procedura di consenso; per le licenze per imprese e hotel, i figli dei dipendenti o degli ospiti e i coordinatori dell'organizzazione.
Dati personali — alunni (sito web, in una classe)	Nome o soprannome inserito dall'alunno o dall'insegnante (da 2 a 24 caratteri; dalle importazioni di elenchi, nome e iniziale, estesa al massimo alle prime 3 lettere del cognome solo per distinguere due alunni con lo stesso nome — mai il nome completo); fascia d'età scelta nel gioco (9–12 o 13–17); avatar da un insieme fisso; lingua; progressi (punti, obiettivi e missioni completati, stelle del quiz, numero di domande risposte e corrette per argomento); compiti completati; data di iscrizione e dell'ultima attività; un token di classe casuale memorizzato sul dispositivo dell'alunno affinché i progressi possano essere salvati. In un quiz di classe dal vivo: il soprannome inserito, le risposte, i tempi di risposta e il punteggio. Non sono raccolti: indirizzo e-mail, cognome, fotografia, data di nascita, indirizzo postale, posizione, identificativi del dispositivo o pubblicitari.

Voce	Descrizione
Dati personali — alunni (avvii LTI)	Un hash con chiave dell'identificativo utente della piattaforma (per associare un alunno a un posto); l'identificativo utente della piattaforma nel record di avvio per 90 giorni, solo quando la piattaforma ha concesso il servizio di valutazione (necessario per la restituzione dei punteggi); nome e iniziale del cognome come soprannome; identificativo e titolo del corso; ruoli; impostazioni locali; ultimo punteggio inviato. Non vengono memorizzati né l'indirizzo e-mail né il nome completo; il Titolare configura la propria piattaforma affinché condivida solo il nome.
Dati personali — alunni (app mobile, pannello di classe)	Attività (gioco quotidiano giocato, data, lingua, punti, completamento, durata; obiettivi raggiunti, badge) e un hash unidirezionale di un identificativo di installazione casuale generato dall'app. Gli alunni compaiono all'insegnante con uno pseudonimo generato. Il pannello non mostra nulla per una classe con meno di cinque alunni attivi.
Dati personali — alunni (studio di impatto, quando il Titolare iscrive una classe)	Risposte al questionario dello studio (scelte, valutazioni e brevi risposte facoltative a testo libero), versione del questionario, lingua, fascia d'età, orari di inizio e di invio e indicatori di qualità. Gli indirizzi e-mail e i numeri di telefono vengono rimossi dal testo libero al ricevimento. Le risposte che possono contenere una rivelazione rilevante per la tutela dei minori sono segnalate al referente nominato dal Titolare. Le risposte sono collegate tra le rilevazioni dello studio da un hash unidirezionale con chiave del posto dell'alunno nella classe; non vengono raccolti nome, indirizzo e-mail né data di nascita. Per ogni posto, l'opposizione o il consenso scritto registrato dal Titolare. Se non è nominato un referente per la tutela dei minori, ne prendono il posto i destinatari indicati nella clausola 4.4.
Dati personali — insegnanti e amministratori scolastici	Nome, indirizzo e-mail di lavoro, scuola, ruolo (insegnante o amministratore scolastico), lingua; password (hash bcrypt) o identificativo di accesso unico; segreto dell'autenticazione a due fattori e codici di recupero sottoposti a hash se attivata (obbligatoria per gli amministratori scolastici); stato di verifica dell'e-mail; orari e numero di accessi; sessioni; classi create; anteprime delle importazioni di elenchi (solo nomi, conservate nella sessione per 30 minuti); voci del registro di audit delle azioni amministrative (con un hash con chiave dell'indirizzo IP e il paese della connessione come codice di 2 lettere fornito dalla rete di distribuzione dei contenuti); corrispondenza di assistenza.
Dati personali — insegnanti (studio di impatto)	Risposte al questionario per gli insegnanti e, per gli alunni di 6–8 anni, la scheda di osservazione della classe, collegate da un hash unidirezionale con chiave dell'account o del codice dell'insegnante; l'iscrizione della classe, la sua modalità di consenso e la sua assegnazione a un gruppo dello studio.
Dati personali — genitori e tutori	Solo quando si utilizza la procedura di consenso parentale del sito web per un alunno al di sotto dell'età del consenso digitale: un hash unidirezionale con chiave dell'indirizzo e-mail del genitore (l'indirizzo stesso è utilizzato una sola volta per inviare il link di conferma e non viene memorizzato), la decisione e le relative marche temporali.

Voce	Descrizione
Dati personali — bambini e coordinatori (licenze per imprese e hotel)	Figli dei dipendenti o degli ospiti del Titolare: si uniscono a un gruppo con il codice di accesso del Titolare e un nome da eroe (soprannome) sul proprio dispositivo o su quello di famiglia, senza account e senza indirizzo e-mail. Il Servizio conserva gli stessi dati degli alunni di una classe: nome da eroe, fascia d'età, avatar, lingua, progressi e risultati dei quiz. Coordinatori: nome, indirizzo e-mail di lavoro, hash della password o identificativo di accesso, impostazioni dell'autenticazione a due fattori e i gruppi che aprono. Il coordinatore vede gli obiettivi completati e i risultati dei quiz per gruppo e può esportarli in CSV. Per il report dell'organizzazione, il Servizio registra inoltre, per ogni profilo eroe di questi gruppi, i giorni di attività e il giorno in cui ogni obiettivo o missione è stato completato per la prima volta (con precisione al giorno; le classi delle scuole non vengono registrate così). I report contengono solo dati aggregati: nessun nome, soprannome, identificativo o riga per bambino; ogni dato basato su 1-4 famiglie viene nascosto (k = 5), e un secondo dato viene nascosto quando uno solo permetterebbe di ricavarlo. I nomi delle squadre sono scelti dall'amministratore del Titolare e non devono nominare persone. Quando il Titolare attiva l'accesso aziendale, i nomi e gli indirizzi e-mail del personale provengono dal provider di identità del Titolare stesso (ambiti openid, email e profile); tale provider è un sistema e un responsabile del Titolare stesso, non un Sub-responsabile, e il suo identificativo del soggetto viene conservato solo come hash con chiave. Co-branding: il nome visualizzato e il logo dell'organizzazione, forniti dal Titolare. La pagina pubblica del badge che un genitore o tutore può condividere su LinkedIn non contiene dati personali (un numero di obiettivi, il nome dell'organizzazione se il Titolare ha aderito, e una lingua, tutto ricavato dal suo link); la condivisione la avvia l'adulto, e il Responsabile non invia nulla a LinkedIn.
Categorie particolari (articolo 9 del RGPD)	Nessuna è richiesta o necessaria. Si veda la clausola 4.2.
Frequenza	Continua, per la durata della Licenza.

B. Trattamenti di cui Eco Heroes è titolare autonomo (fuori dal presente Accordo)

Elencati affinché il Titolare veda dove termina il presente Accordo. Sono disciplinati dall'Informativa sulla privacy (v4.3) e dall'Informativa sulla privacy dei minori (v2.2) del Responsabile, non dal presente Accordo:

- **Gli account insegnante in quanto tali:** accesso, sicurezza, autenticazione a due fattori e risorse gratuite per insegnanti. Il Responsabile è titolare dell'account in sé e lo cancella come previsto dalla clausola 10.4; l'attività dell'account per il Titolare costituisce Dati del Titolare.
- **Account insegnante gratuiti:** insegnanti non collegati a una licenza che utilizzano le risorse gratuite per insegnanti con un indirizzo e-mail verificato.
- **Abbonamenti familiari** sul sito web, sottoscritti da un genitore o tutore: l'indirizzo e-mail (memorizzato parzialmente mascherato), i riferimenti di pagamento e di abbonamento Stripe e un codice di accesso personale (memorizzato come hash con chiave). I dati della carta non raggiungono mai il Responsabile. Un codice familiare utilizzato a scuola non porta con sé dati della scuola.
- **Account dell'app** (accesso dei genitori con Google o Apple; abbonamenti tramite Google Play o Apple; stato dell'abbonamento tramite RevenueCat).
- **Visitatori del sito web** sulle pagine pubbliche per adulti (Google Analytics 4 previo consenso; il modulo di contatto tramite Formspree; le richieste di preventivo e le candidature ad ambasciatore tramite il server proprio del Responsabile; le e-mail Dinner Questions tramite Brevo).

- **Classifica pubblica del quiz** (facoltativa: un soprannome scelto da un elenco generato, il punteggio e un hash con chiave dell'indirizzo IP; conservati 30 giorni).
- **Sondaggi del programma** che il Responsabile svolge al di fuori di una classe, con il consenso di un genitore ove la legge lo richieda.
- **Servizi distinti:** Eco Heroes Academy (learn.eco-heroes.org) e la valutazione VSME (assessment.eco-heroes.org) hanno propri termini e informative sulla privacy.

C. Calendario di conservazione (come applicato nel Servizio)

Allegato I.C — calendario di conservazione

Dati	Conservazione	Meccanismo
Dati degli alunni e dei bambini dei gruppi di imprese e hotel (soprannome, fascia d'età, avatar, progressi, compiti, attività di classe nell'app, associazione dei posti LTI)	Durante la Licenza: finché un insegnante o un amministratore cancella l'alunno o la classe. Dopo la fine della Licenza: cancellazione 90 giorni dopo la data di cessazione, salvo rinnovo della Licenza. Su richiesta scritta del Titolare: cancellazione entro 30 giorni; gli amministratori scolastici ricevono un avviso via e-mail 30 e 7 giorni prima della cancellazione	Azione dell'insegnante o dell'amministratore nel Servizio; cancellazione automatica a fine licenza; il Responsabile su richiesta scritta
Date di attività dei profili eroe nei gruppi aziendali e degli hotel (report dell'organizzazione)	Conservate con il profilo eroe e cancellate insieme a esso, secondo la regola qui sopra	Cancellazione con il profilo
Impostazioni dell'organizzazione: nomi delle squadre e squadra di ogni gruppo, attivazione della classifica a squadre, nome e logo del co-branding, configurazione dell'accesso aziendale	Per la durata della Licenza; cancellate su richiesta del Titolare	Responsabile, su richiesta
Accesso aziendale: registrazioni della procedura di accesso; collegamenti di identità fissati (hash con chiave del soggetto del provider di identità)	Registrazioni della procedura: cancellate all'uso o dopo 10 minuti. Collegamenti di identità: finché l'account non viene cancellato o la configurazione di accesso del Titolare non viene rimossa o reimpostata	Pulizia automatica; azione di un amministratore
Quiz di classe dal vivo (soprannomi, risposte, tempi, punteggi)	30 giorni dalla creazione della sessione del quiz	Pulizia giornaliera automatica
Anteprime delle importazioni di elenchi (OneRoster)	30 minuti, solo nella sessione server dell'insegnante	Scadenza della sessione
Token di accesso Google Classroom (importazione di elenchi)	Solo durante l'importazione, nella sessione dell'insegnante; mai scritto nel database	Scadenza della sessione
Record di avvio LTI	Avvii degli insegnanti, e avvii degli alunni senza servizio di valutazione: 2 ore. Avvii degli alunni con servizio di valutazione: 90 giorni	Pulizia automatica durante l'attività LTI

Dati	Conservazione	Meccanismo
Stato di accesso LTI, token di passaggio, token di deep linking, nonce, token di importazione degli elenchi	10 minuti / 10 minuti / 60 minuti / 15 minuti / 2 ore	Pulizia automatica; uso singolo
Account di insegnanti, coordinatori e amministratori scolastici	12 mesi dopo la fine dell'ultima licenza collegata all'account; account gratuiti dopo 12 mesi senza accessi; e-mail di avviso 30 giorni prima della cancellazione. Registrazioni non verificate: cancellate 7 giorni dopo la scadenza dell'ultimo link di conferma	Pulizia automatica degli account
Sessioni e «ricordami»	Sessione server per la durata configurata, rinnovata all'accesso e ogni 30 minuti; tutte le sessioni terminano al cambio della password o quando un amministratore revoca l'accesso. Cookie «ricordami»: 180 giorni (firmato HMAC)	Codice
Record di limitazione delle richieste (tentativi di accesso e altri limiti)	30 giorni	Pulizia giornaliera automatica
Registro di audit di sicurezza (azioni amministrative, attivazioni di codici e accessi; hash con chiave dell'IP, paese della connessione come codice di 2 lettere)	12 mesi	Pulizia giornaliera automatica
Hash IP anti-abuso sulle risposte ai sondaggi e sulle richieste di consenso	30 giorni (la risposta stessa segue il proprio periodo)	Pulizia giornaliera automatica
Richieste di consenso parentale	Senza risposta o scadute: 30 giorni. Rifiuti: 12 mesi. Consenso prestato: finché vi si fa affidamento; cancellato insieme ai dati in caso di revoca del consenso	Pulizia giornaliera automatica; funzione di cancellazione
Risposte agli studi di impatto (alunni, insegnanti, schede di osservazione) e indicatori di opposizione o di consenso	24 mesi dopo la chiusura dell'ultima rilevazione dello studio; prima su istruzione scritta del Titolare. Gli indicatori di opposizione e di consenso sono cancellati insieme all'iscrizione della classe	Pulizia giornaliera automatica; il Responsabile su richiesta scritta
Segnalazioni di tutela dei minori (risposte agli studi di impatto che possono contenere una rivelazione, con il posto e il soprannome a cui si riferiscono)	Il testo della risposta è cancellato 30 giorni dopo che la segnalazione è stata segnata come gestita; la registrazione della segnalazione è cancellata 12 mesi dopo la gestione	Pulizia giornaliera automatica
Risposte ai sondaggi del programma	24 mesi, o fino alla revoca del consenso	Pulizia giornaliera automatica; funzione di cancellazione

Dati	Conservazione	Meccanismo
Voci della classifica pubblica del quiz (fuori dal presente Accordo, elencate per completezza)	30 giorni	Pulizia giornaliera automatica
Registrazioni dell'accettazione del presente Accordo da parte del Titolare (chi l'ha accettato, quando, quale versione, hash con chiave dell'indirizzo IP; conservate dal Responsabile in qualità di titolare, clausola 13.3)	Per tutta la durata della Licenza e 6 anni dopo la sua fine	Registri del Responsabile
Registrazioni dell'accettazione al pagamento, delle disdette e dei recessi dei piani famiglia (fuori dal presente Accordo, elencate per completezza)	6 anni, con le scritture contabili (Codice di commercio spagnolo, articolo 30)	Scritture contabili
Contatore del tasso di partecipazione derivato da una persona	2 giorni	Pulizia giornaliera automatica
Telemetria (segnalazioni di violazioni CSP ed errori JavaScript)	Nessun identificativo memorizzato (user agent troncato); contatori di limitazione azzerati ogni minuto; registro limitato a 5 MB	Codice
Corrispondenza di assistenza (e-mail)	Fino alla gestione della richiesta, e al massimo 12 mesi dopo l'ultimo messaggio	Procedura della casella di posta del Responsabile
Backup cifrati	Backup cifrati conservati a rotazione; i dati cancellati escono da tutti i backup entro 14 giorni	Automatico
Replica di riserva del database	Continua; recepisce ogni cancellazione	Replica
Log tecnici del server web (indirizzo IP, indirizzo richiesto)	Fino a 90 giorni	Configurazione del server
Fatture e documenti di pagamento	6 anni (Codice di commercio spagnolo, articolo 30); identificano le persone di contatto del Titolare, mai gli alunni	Scritture contabili

Allegato II — Misure tecniche e organizzative (articolo 32 del RGPD)

Le misure in essere alla data del presente Accordo. Sono riesaminate a ogni rilascio, e la sintesi vigente è pubblicata all'indirizzo https://eco-heroes.org/trust/#security. Il Responsabile può aggiornare le misure purché il livello complessivo di sicurezza non diminuisca.

1. Cifratura in transito

- TLS 1.2 o superiore per tutte le connessioni; HTTP Strict Transport Security con max-age di due anni, includeSubDomains e preload; rinnovo automatico dei certificati; certificati di origine tra la rete di distribuzione dei contenuti e i server.
- I server applicativi si connettono al database solo tramite TLS 1.2/1.3, con verifica del certificato rispetto a un'autorità di certificazione fissata; il database rifiuta le connessioni non cifrate (require_secure_transport). Gli account del database sono limitati agli host applicativi e di riserva.
- I backup sono cifrati (AES-256-CBC, PBKDF2 con 200.000 iterazioni) prima di lasciare il server e transitano solo su connessioni cifrate. Non vengono scritti archivi non cifrati.

2. Protezione lato browser

- Content-Security-Policy: gli script inline vengono eseguiti solo se approvati da un hash SHA-256 per script, o da un nonce per richiesta su alcune pagine dinamiche (nessun unsafe-inline per gli script — gli stili inline restano consentiti; object-src 'none', base-uri 'self', frame-ancestors 'none' tranne che per le pagine LTI, che solo le piattaforme di apprendimento registrate possono incorporare). Le segnalazioni di violazione sono raccolte con limitazione delle richieste. Le pagine per bambini non caricano script di terzi. Sulle pagine per adulti, gli unici script di terzi sono Google Analytics, previo consenso, e la verifica Cloudflare Turnstile sui moduli di accesso e di registrazione.
- I font web sono ospitati sul server proprio del Responsabile. Non viene inviata alcuna richiesta a Google Fonts né ad altri fornitori di font.
- Intestazioni di sicurezza: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy e Cross-Origin-Resource-Policy same-origin. Le intestazioni di versione del server e di PHP sono rimosse. HTTP TRACE e TRACK sono rifiutati.
- Cookie: il cookie di sessione è Secure, HttpOnly e SameSite=Strict, in modalità di sessione rigorosa; l'identificativo di sessione cambia all'accesso, all'attivazione di un codice e ogni 30 minuti. Il cookie «ricordami» è firmato HMAC con una chiave lato server. Il cookie di stato LTI è limitato a /lti/ e partizionato.
- Il service worker dei giochi non memorizza mai nella cache le risposte contrassegnate no-store o private né alcun percorso riservato ai membri, cosicché nessun contenuto riservato resta nella cache di un dispositivo condiviso dopo la disconnessione.
- Le risposte contenenti dati personali o contenuti riservati ai membri sono inviate con Cache-Control: private, no-store, e la rete di distribuzione dei contenuti non le memorizza mai nella cache.

3. Controllo degli accessi e autenticazione

- Account insegnante nominativi: un codice scuola è utilizzato una sola volta, per l'iscrizione. Crea un account nominativo con un indirizzo e-mail verificato, oppure collega la scuola all'account che l'insegnante ha già. In seguito l'insegnante accede con il proprio indirizzo e-mail e la propria password, o tramite accesso unico. Un dispositivo su cui è stato inserito solo un codice scuola può giocare, ma non ha gli strumenti per insegnanti. Un codice di amministrazione crea solo il primo account di

amministrazione della scuola e si esaurisce quando tale account è confermato; gli insegnanti si uniscono poi con un codice del personale che un amministratore scolastico crea nel Servizio, mostrato una sola volta, memorizzato solo come hash con chiave e sostituibile in qualsiasi momento.

- Le password degli insegnanti sono sottoposte a hash con bcrypte confrontate in tempo costante. L'indirizzo e-mail deve essere verificato prima del primo accesso. Il cambio della password termina tutte le sessioni. Un amministratore scolastico può revocare immediatamente l'accesso di un insegnante.
- L'autenticazione a due fattori (TOTP, con codici di recupero sottoposti a hash) è obbligatoria per gli amministratori scolastici e per i super amministratori del Responsabile, e qualsiasi insegnante o coordinatore di una licenza aziendale o alberghiera può attivarla. Il codice QR di registrazione è generato sul server, cosicché il segreto non lo lascia mai. Il secondo fattore è verificato prima che venga creata qualsiasi sessione, e gli amministratori scolastici devono usarlo ovunque siano visibili dati degli alunni. Anche il referente per la tutela dei minori deve usarlo per leggere le segnalazioni di tutela. Dopo 10 codici errati in 24 ore, il secondo fattore dell'account viene bloccato per 15 minuti e il titolare dell'account viene avvisato via e-mail.
- I codici di accesso sono memorizzati solo come hash con chiave in un file al di fuori della radice web; la chiave è conservata al di fuori della radice web. I codici di registrazione e di licenza sono memorizzati allo stesso modo; un codice è mostrato una sola volta, quando viene creato.
- Limitazione delle richieste su accesso (per indirizzo IP e per coppia e-mail/IP, con un tetto globale), registrazione, riscatto dei codici, ingresso in una classe, ingresso in un quiz dal vivo, sincronizzazione dei progressi, modulo di preventivo, accessi LTI, endpoint di telemetria e consultazioni di ritorno da Stripe. Token CSRF su ogni modulo che modifica dati. Protezione dai reindirizzamenti aperti su ogni parametro next=.
- Diritti di accesso verificati lato server: le risorse riservate ai membri (video delle missioni, banche di domande del quiz, libri, contenuti LTI) sono servite solo dopo che il server ha verificato una sessione di codice valida, un codice memorizzato firmato o un account connesso. Nulla di ciò che il browser scrive da sé concede l'accesso.
- Isolamento per ruolo e per scuola: ogni insegnante vede solo le proprie classi; gli amministratori scolastici vedono tutte le classi della propria scuola e nulla delle altre scuole; gli insegnanti che arrivano tramite LTI vedono solo le classi del corso da cui sono partiti; l'accesso da super amministratore è limitato al personale del Responsabile nominativamente individuato.
- Tutte le query al database utilizzano istruzioni preparate; nessun exec, eval o unserialize; i percorsi dei file sono costruiti solo da elementi di un elenco consentito; i caricamenti (file CSV/ZIP degli elenchi, immagini dei sondaggi) sono limitati in dimensione, controllati nel tipo e memorizzati al di fuori della radice web; la visualizzazione degli errori PHP è disattivata.
- Single sign-on facoltativo per il personale di aziende e hotel tramite OpenID Connect (Authorization Code con PKCE; token di identità firmati e verificati per emittente, destinatario, scadenza e nonce). I segreti client sono cifrati a riposo. Gli account vengono associati solo all'interno dei domini e-mail autorizzati del Titolare e non vengono mai collegati all'account di un'altra organizzazione.

4. Minimizzazione dei dati e dati dei minori

- Non vengono raccolti indirizzi e-mail, cognomi, fotografie, date di nascita, indirizzi postali, posizioni né identificativi del dispositivo o pubblicitari degli alunni. Le importazioni di elenchi conservano il nome e al massimo le prime 3 lettere del cognome. Gli alunni che arrivano tramite LTI sono memorizzati con un hash con chiave dell'identificativo utente della piattaforma, con nome e iniziale; il Titolare configura la propria piattaforma affinché condivida solo il nome.

- Gli indirizzi IP sono memorizzati solo come hash con chiave (prefisso). Chi detiene la chiave potrebbe ricollegarli; sono quindi pseudonimizzati, non anonimi. Quando accompagnano un contenuto, sono cancellati dopo 30 giorni.
- Le pagine per bambini (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books e le loro versioni linguistiche) non caricano strumenti di analisi e non mostrano un banner di consenso. Sulle altre pagine, l'analisi si carica solo dopo un consenso esplicito.
- I video delle missioni riservati ai membri sono ospitati dal Responsabile e serviti dopo la verifica dei diritti di accesso. Dove resta un lettore YouTube (gioco libero), utilizza youtube-nocookie.com e si carica solo quando l'utente preme riproduci.
- La pubblicazione nella classifica pubblica del quiz è facoltativa dopo ogni partita, con un soprannome generato (un aggettivo e un animale; nessun testo libero né nome di scuola). La classifica pubblica mostra soprannome e punteggio dei primi 10 degli ultimi 30 giorni, e le voci sono cancellate dopo 30 giorni. Ogni riga pubblica ha un link per la segnalazione; una riga segnalata tre volte viene nascosta fino alla revisione. Le classifiche di classe sono visibili solo all'insegnante di quella classe e agli amministratori della scuola, che possono rimuovere righe.
- Le risposte a testo libero sono filtrate automaticamente all'invio: gli indirizzi e-mail e i numeri di telefono vengono rimossi, e le risposte che corrispondono a un breve elenco di parole che possono indicare che un bambino è in pericolo sono tolte dai dati dello studio e trasmesse solo al referente per la tutela dei minori designato dalla scuola. I nomi non vengono rimossi automaticamente; i ricercatori che leggono le risposte segnalano i possibili nomi e non li riportano mai. Una possibile rivelazione è trasmessa al referente designato dalla scuola entro un giorno di scuola. Se non è nominato un referente per la tutela dei minori, ne prendono il posto i destinatari indicati nella clausola 4.4.
- Gli indirizzi e-mail dei genitori nella procedura di consenso non sono mai memorizzati in chiaro; si conserva solo un hash con chiave.
- I report dell'organizzazione sono aggregati: un dato basato su meno di 5 famiglie viene nascosto già nel calcolo, così né lo schermo né il CSV possono mostrarlo. Solo gli amministratori dell'organizzazione, con accesso a due fattori, possono aprirli; ogni consultazione ed esportazione ha un limite di frequenza ed è registrata.

5. Disponibilità, backup e ripristino

- Le seguenti operazioni sono eseguite automaticamente. Un monitoraggio indipendente (UptimeRobot, 11 controlli, ogni 5 minuti) avvisa il Responsabile in caso di errore.
- Ogni notte un backup cifrato del database e dell'applicazione; una copia è conservata in un data center separato in un altro Paese dell'UE. Ogni mese viene provato automaticamente un ripristino.
- Un backup prima di ogni rilascio, con una procedura di ritorno alla versione precedente verificata; la versione di produzione precedente è conservata.
- Un server di riserva contiene una copia dell'applicazione e una replica attiva del database. Se il server web principale si guasta, un bilanciamento del carico con controlli di stato sposta il traffico automaticamente; se si guasta il server del database, la replica viene promossa con una procedura scriptata e provata. Entrambi sono stati testati nell'ottobre 2026.
- Un controllo orario dell'infrastruttura (stato e ritardo della replica, scadenza dei certificati, spazio su disco, aggiornamenti di sicurezza in sospeso, intervalli di indirizzi della rete di distribuzione dei contenuti). Gli aggiornamenti di sicurezza del sistema operativo si installano automaticamente. Protezione da attacchi DDoS e bot ai margini della rete.

- L'ambiente di staging è separato dalla produzione (utente Unix distinto, pool PHP con open_basedir, istanza di database distinta, segreti rimossi).

6. Registrazione e monitoraggio

- Gli eventi di sicurezza (accessi falliti, riscatti di codici, azioni amministrative, segnalazioni di violazione CSP, cancellazioni e pulizie di conservazione) sono registrati con hash con chiave degli indirizzi IP. Il registro di audit di sicurezza è conservato 12 mesi e i record di limitazione delle richieste 30 giorni (Allegato I, sezione C).
- Lo stato del servizio in tempo reale e ogni interruzione sono pubblicati sulla pagina di stato pubblica.

7. Misure organizzative

- L'accesso ai sistemi di produzione è limitato a persone nominativamente individuate. Ogni account amministrativo (hosting, server del database e dei backup, rete di distribuzione dei contenuti e DNS, repository del codice sorgente, monitoraggio, posta elettronica) utilizza l'autenticazione a due fattori. L'accesso ai server avviene con chiavi SSH. I firewall limitano l'accesso al database e al server di riserva agli host propri del Responsabile e agli intervalli di indirizzi della rete di distribuzione dei contenuti.
- Le modifiche sono verificate automaticamente (integrazione continua; un rilascio è rifiutato se il codice non ha superato i test), passano prima per lo staging e sono verificate in produzione dopo ogni rilascio (47 controlli dal vivo). Una revisione statica di sicurezza dell'applicazione è svolta e documentata (l'ultima: 16 ottobre 2026).
- Penetration test, ottobre 2026: un test strutturato white-box e grey-box della piattaforma (autenticazione, sessioni, controllo degli accessi tra scuole, pagamenti, esposizione di file e dati, limitazione dei tentativi e cache perimetrale), svolto dal team di test interno del Responsabile. Tutte le vulnerabilità critiche, alte e medie riscontrate sono state corrette e verificate di nuovo prima del rilascio. È previsto un penetration test esterno, affidato a una società indipendente.
- Un canale di segnalazione delle vulnerabilità è pubblicato all'indirizzo /.well-known/security.txt. Le segnalazioni ricevono un avviso di ricevimento entro 5 giorni lavorativi e i problemi critici vengono risolti prima di qualsiasi altro lavoro.
- Una procedura scritta di gestione degli incidenti descrive come il Responsabile rileva, contiene e documenta una violazione dei dati personali e come rispetta il termine di notifica di 48 ore della clausola 9.
- Il Responsabile tiene un registro dei trattamenti che svolge per conto dei titolari (articolo 30, paragrafo 2, del RGPD) e una valutazione del trasferimento per ciascun Sub-responsabile al di fuori del SEE.
- I periodi di conservazione sono definiti nel codice che li applica, cosicché il periodo pubblicato e quello applicato non possono divergere.
- I segreti (chiave limitata di Stripe, credenziali di accesso unico, chiavi di hash) sono conservati al di fuori della radice web e non vengono mai inseriti nel repository del codice sorgente.

Allegato III — Sub-responsabili e servizi di terzi

Il Trust Centre (https://eco-heroes.org/trust/#subprocessors) mostra gli stessi due elenchi.

Parte A — Sub-responsabili che trattano Dati del Titolare

Allegato III.A — sub-responsabili autorizzati

Sub-responsabile	Che cosa fa	Dove	Garanzia per il trasferimento
Internet Girona, su infrastruttura OVHcloud	Hosting web	Francia (UE)	Nell'UE; condizioni standard di trattamento dei dati del fornitore
Hetzner Online GmbH, Gunzenhausen, Germania	Hosting del database, server di riserva e backup cifrati	Germania e Finlandia (UE)	Nell'UE; condizioni standard di trattamento dei dati di Hetzner
Cloudflare, Inc., San Francisco, USA	Distribuzione dei contenuti, TLS, protezione da attacchi e bot, verifica Turnstile sui moduli di accesso e di registrazione, e failover automatico	Rete periferica globale; server di origine nell'UE	Condizioni standard di trattamento dei dati di Cloudflare con le clausole contrattuali tipo (2021/914); quadro UE-USA per la protezione dei dati personali se Cloudflare è in elenco
Proton AG, Ginevra, Svizzera	Hosting della posta info@ e security@eco-heroes.org: corrispondenza di assistenza e sulla protezione dei dati con il personale del Titolare	Svizzera	Decisione di adeguatezza della Commissione europea per la Svizzera; condizioni standard di trattamento dei dati di Proton
Google (Google Ireland Ltd / Google LLC) — solo accesso e importazione Classroom	Solo se il Titolare li attiva: accesso degli insegnanti (nome, indirizzo e-mail, identificativo; nessun dato degli alunni); importazione degli elenchi Google Classroom (nome e cognome letti una volta e memorizzati come nome e iniziale; il token di accesso resta nella sessione dell'insegnante)	UE / USA	Termini Google propri del Titolare; condizioni standard di trattamento dei dati di Google con le clausole contrattuali tipo; quadro UE-USA per la protezione dei dati personali se in elenco
Microsoft (Microsoft Ireland Operations Ltd) — solo accesso	Solo se il Titolare lo attiva: accesso degli insegnanti (solo identità; nessun dato degli alunni)	UE / USA	Termini Microsoft propri del Titolare; Microsoft Products and Services DPA con le clausole contrattuali tipo; quadro UE-USA per la protezione dei dati personali se in elenco

Sub-responsabile	Che cosa fa	Dove	Garanzia per il trasferimento
Google (YouTube, youtube-nocookie.com)	Riproduzione di video didattici selezionati dove è ancora utilizzato un lettore YouTube: modalità di privacy avanzata, caricata solo quando l'utente preme riproduci	UE / USA	Termini di Google; quadro UE-USA per la protezione dei dati personali se in elenco
Moodle Pty Ltd (MoodleCloud), Australia Occidentale	Solo se il Titolare utilizza il sito dei corsi Eco Heroes eco-heroes.moodlecloud.com invece della propria piattaforma di apprendimento: account dei corsi su quel sito e progressi che i giochi vi comunicano	Hosting MoodleCloud su Amazon Web Services	Accordo sul trattamento dei dati di MoodleCloud con le clausole contrattuali tipo (2021/914) per ogni trasferimento al di fuori del SEE

Parte B — Servizi di terzi che non trattano Dati del Titolare

Elencati per trasparenza. Ove siano coinvolti dati personali, si applica l'Informativa sulla privacy del Responsabile. Il server di posta proprio del Responsabile invia le e-mail di account, di verifica e di servizio; non è un terzo.

Allegato III.B — servizi di terzi fuori dal presente Accordo

Servizio	Che cosa fa	Dove	Perché è fuori dal presente Accordo
Stripe	Pagamenti con carta degli abbonamenti familiari sul sito web; il Responsabile legge lo stato del pagamento e dell'abbonamento	UE / USA; condizioni di trattamento dei dati di Stripe con le clausole contrattuali tipo; quadro UE-USA per la protezione dei dati personali	Gli abbonati familiari sono clienti propri del Responsabile; nessun dato della scuola è inviato a Stripe
Google Analytics 4	Statistiche di visita sulle pagine pubbliche per adulti, solo previo consenso; mai sulle pagine per bambini né nell'area insegnanti	UE / USA; condizioni di trattamento dei dati di Google con le clausole contrattuali tipo; quadro UE-USA per la protezione dei dati personali	Non vengono inviati Dati del Titolare; il Responsabile è titolare delle proprie statistiche web
Formspree	Inoltra i messaggi inviati con il modulo di contatto generale	USA; condizioni standard di trattamento dei dati del fornitore (clausole contrattuali tipo; quadro UE-USA per la protezione dei dati personali se in elenco)	I messaggi sono corrispondenza propria del Responsabile; non utilizzato dal Servizio
Brevo	E-mail Dinner Questions per le famiglie (su iscrizione; solo indirizzo e-mail)	UE	Newsletter per le famiglie; non utilizzata dal Servizio
RevenueCat	Stato dell'abbonamento nell'app (solo identificativo dell'account e cronologia degli acquisti)	USA; clausole contrattuali tipo	Account familiari dell'app; nessun dato della scuola

Servizio	Che cosa fa	Dove	Perché è fuori dal presente Accordo
Google Play / Apple App Store	Pagamenti degli abbonamenti nell'app, riscossi dallo store	UE / USA	Gli store vendono l'abbonamento in qualità di titolari autonomi
Google / Apple (accesso nell'app)	Accesso facoltativo dei genitori nell'app (indirizzo e-mail e identificativo di accesso)	UE / USA; quadro UE-USA per la protezione dei dati personali, clausole contrattuali tipo	Account familiari dell'app; nessun dato della scuola
UptimeRobot	Verifica che le pagine pubbliche e l'endpoint di stato rispondano	UE / USA	Non tratta dati personali

Allegato IV — Dati dei minori

Il presente allegato integra gli Allegati I e II per gli alunni di età inferiore a 18 anni.

1. **Età del consenso digitale.** Se la legge applicabile al Titolare richiede il consenso per i servizi della società dell'informazione offerti direttamente a un minore (articolo 8 del RGPD), il Titolare lo ottiene e lo registra. Tale età è di 14 anni in Spagna (articolo 7 della LOPDGDD), tra 13 e 16 anni negli altri Stati membri dell'UE e di 13 anni nel Regno Unito; per le scuole negli Stati Uniti si veda l'Allegato V. Se il Titolare si basa su un'altra base giuridica per l'uso scolastico, per esempio un compito di interesse pubblico, non è necessario alcun consenso e il Titolare informa alunni e genitori. Il Servizio non verifica l'età. Le sue due fasce d'età (9–12 e 13–17) selezionano solo i contenuti e la versione dei video.
2. **Procedura di consenso parentale sul sito web.** Quando una funzione del sito web richiede il consenso di un genitore per un minore al di sotto dell'età del consenso digitale, il Servizio non memorizza nulla finché il genitore non conferma tramite un link monouso inviato via e-mail. Sono memorizzati solo un hash con chiave dell'indirizzo e-mail del genitore, la decisione e le marche temporali. Le richieste senza risposta sono cancellate dopo 30 giorni e i rifiuti dopo 12 mesi. La revoca del consenso cancella i dati raccolti in base a esso.
3. **Piano famiglia.** Un genitore o tutore sottoscrive l'abbonamento familiare ed è cliente del Responsabile. Sul sito web, il pagamento chiede all'acquirente di confermare di essere maggiorenne; nell'app, i passaggi di accesso e di acquisto si trovano dietro una verifica per adulti (una domanda di aritmetica a cui rispondere digitando). Nessuna delle due è una verifica dell'identità o dell'età. I bambini non aprono account sul sito web. Un bambino può utilizzare un codice familiare sotto la responsabilità del genitore; ad esso non sono collegati dati della scuola.
4. **Nessuna profilazione né pubblicità.** Il Responsabile non mostra pubblicità e non utilizza identificativi o SDK pubblicitari. Non crea profili degli alunni oltre al monitoraggio dei progressi che vedono gli insegnanti del Titolare, non prende decisioni automatizzate che producano effetti giuridici o effetti analogamente significativi e non vende né condivide mai dati degli alunni per pubblicità.
5. **Nessuna analisi sulle pagine per bambini.** Le pagine per bambini (il gioco di avventura, l'area giochi, il quiz, la biblioteca, le pagine degli obiettivi, Wordle, le missioni e i libri, in tutte le 13 lingue) non caricano strumenti di analisi, tracker né banner di consenso. Utilizzano solo la memoria del browser strettamente necessaria (lingua, progressi sul dispositivo, sessione).
6. **Studi di impatto.** Quando il Titolare iscrive classi a uno studio di impatto, gli alunni rispondono in classe nell'ambito della valutazione che il Titolare fa del proprio insegnamento. Il Titolare informa i genitori in anticipo e offre loro la possibilità di opporsi, oppure raccoglie un consenso scritto ove la sua legge o le sue regole lo richiedano; il Servizio supporta entrambe le modalità ed esclude i posti interessati. Gli alunni possono saltare qualsiasi domanda e ne sono informati nella prima schermata. Gli insegnanti vedono solo risultati di classe, e solo quando almeno 10 alunni hanno risposto prima e dopo; nessun utente della scuola vede le risposte individuali di un alunno. Una risposta a testo libero che può contenere una rivelazione rilevante per la tutela dei minori è inoltrata al referente nominato dal Titolare, che decide come procedere. Il Responsabile utilizza solo risultati aggregati e anonimizzati ai sensi della clausola 2.3, mai testo libero. Una possibile rivelazione è trasmessa al referente designato entro un giorno di scuola, e solo quel referente la vede. Se non è nominato un referente per la tutela dei minori, ne prendono il posto i destinatari indicati nella clausola 4.4.
7. **Nessuna funzione di comunicazione.** Il Servizio non ha chat, messaggistica né profili pubblici degli alunni. La classifica pubblica del quiz è facoltativa, utilizza solo soprannomi scelti da un elenco generato, non mostra nomi di scuole, conserva le voci per 30 giorni e ha un link per la segnalazione su

ogni voce. Le classifiche di classe sono visibili solo all'insegnante della classe e agli amministratori della scuola, e una voce pubblica segnalata tre volte viene nascosta fino alla revisione.

8. **Rischio residuo comunicato al Titolare.** Un compagno che conosce un codice classe e il soprannome di un alunno può aprire i progressi di tale alunno su un altro dispositivo. Gli insegnanti possono vedere, rinominare o rimuovere alunni in qualsiasi momento e possono rinnovare il codice classe. Il Titolare ne tiene conto nella propria valutazione e nel modo in cui distribuisce i codici classe.
9. **Diritti dei genitori e degli alunni.** Genitori e alunni esercitano i propri diritti nei confronti del Titolare. Gli insegnanti del Titolare possono visualizzare, esportare, rinominare, azzerare e cancellare direttamente i dati di un alunno. Il Responsabile inoltra al Titolare qualsiasi richiesta riceva (clausola 8.2).
10. **Informazioni per i bambini.** Il Responsabile pubblica un'Informativa sulla privacy dei minori con una parte scritta per i bambini (Parte A) e una parte per genitori e scuole (Parte B) all'indirizzo https://eco-heroes.org/legal/children/. Il Titolare può riprenderla nelle proprie informazioni per alunni e genitori.

Allegato V — Titolari nel Regno Unito e negli Stati Uniti

1. **Regno Unito.** Se il Titolare è stabilito nel Regno Unito, i riferimenti del presente Accordo al RGPD si intendono fatti allo UK GDPR e al Data Protection Act 2018, e l'autorità di controllo competente è l'Information Commissioner's Office (ICO). I Dati del Titolare sono trasferiti dal Regno Unito al SEE in base ai regolamenti di adeguatezza del Regno Unito per il SEE. I trasferimenti successivi verso gli Stati Uniti si basano sull'estensione britannica del quadro UE-USA per la protezione dei dati personali se il fornitore è certificato, oppure sull'UK International Data Transfer Addendum alle clausole contrattuali tipo. Il Responsabile progetta il Servizio tenendo conto dell'Age Appropriate Design Code dell'ICO; la sua sintesi di conformità è nella sezione 11 dell'Informativa sulla privacy.
2. **Stati Uniti — FERPA.** Se il Titolare è una scuola o un distretto scolastico degli Stati Uniti soggetto al Family Educational Rights and Privacy Act, il Responsabile agisce come «school official» con un interesse educativo legittimo ai sensi di 34 CFR 99.31(a)(1)(i)(B). Il Responsabile è sotto il controllo diretto del Titolare per quanto riguarda l'uso e la tenuta dei registri scolastici, li utilizza solo per le finalità della Licenza e non li comunica a nessun altro, salvo ai Sub-responsabili ai sensi della clausola 6 o quando la legge lo richiede.
3. **Stati Uniti — COPPA.** Per gli alunni di età inferiore a 13 anni, il Titolare può prestare il consenso per conto dei genitori alla raccolta dei dati descritti nell'Allegato I, come consentito dalle linee guida della Federal Trade Commission, poiché i dati sono utilizzati solo per le finalità educative del Titolare e per nessun'altra finalità commerciale. Il Titolare tiene informati i genitori e inoltra le loro richieste di visualizzare o cancellare i dati del proprio figlio; il Responsabile vi dà seguito ai sensi della clausola 8.
4. **Stati Uniti — cancellazione e notifica.** Alla cancellazione al termine della Licenza si applica la clausola 10. Se una legge statale sulla privacy degli alunni fissa un termine più breve per la notifica delle violazioni o per la cancellazione, il Responsabile lo rispetta non appena il Titolare gli indica quale legge si applica.
