Aquesta és una traducció facilitada per comoditat. La versió en anglès és el text jurídicament vinculant i prevaldrà en cas de qualsevol discrepància. English (PDF)

Acord d'encàrrec de tractament

d'acord amb l'article 28 del Reglament (UE) 2016/679 (RGPD) i l'article 33 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD) — entre el titular de la llicència (el «Responsable») i Eco Heroes International SL (l'«Encarregat»)

Parts i funcions

Responsable: _____ (denominació del centre educatiu, grup de centres, administració educativa, empresa o hotel indicat a la Llicència), amb domicili social a _____, representat per _____ (nom, càrrec).
Contacte del Responsable per a protecció de dades (contacte administrador o, si se n'ha designat, delegat de protecció de dades): _____.

Encarregat: Eco Heroes International SL, CIF B44915940, amb domicili social a 17003 Girona (Espanya), inscrita al Registre Mercantil de Girona, representada per Karim Zouhdi, fundador. Contacte per a protecció de dades: info@eco-heroes.org, +34 690 814 215. Avisos de seguretat: security@eco-heroes.org (vegeu https://eco-heroes.org/.well-known/security.txt).

Funcions. El Responsable decideix per a què i com es tracten les Dades del Responsable i n'és el responsable del tractament. L'Encarregat tracta les Dades del Responsable únicament per compte del Responsable, com a encarregat del tractament en el sentit de l'article 4.8 del RGPD.

Comptes de docents. Cada docent té un compte personal i nominatiu. L'Encarregat gestiona el compte en si (accés, seguretat, verificació en dos passos i els recursos gratuïts per a docents) com a responsable del tractament, d'acord amb la seva Política de privacitat. Tot el que un docent fa al Servei per al Responsable són Dades del Responsable: el rol i els permisos del compte al centre del Responsable, les classes, l'alumnat, el progrés, les tasques, els qüestionaris en directe, les importacions de llistes de classe, els accessos des de la plataforma d'aprenentatge i els estudis d'impacte.

Fora d'aquest Acord. L'annex I, secció B, enumera els tractaments dels quals l'Encarregat és responsable per si mateix. Aquests tractaments es regeixen per la Política de privacitat de l'Encarregat (https://eco-heroes.org/legal/privacy/), no per aquest Acord. Eco Heroes Academy (learn.eco-heroes.org) i l'avaluació VSME (assessment.eco-heroes.org) són serveis diferents, amb les seves pròpies condicions i informacions de privacitat; aquest Acord no els cobreix.

Aquest Acord forma part de la Llicència. Si la Llicència i aquest Acord es contradiuen pel que fa al tractament de dades personals, preval aquest Acord.

Definicions

- **«Llicència»** significa el contracte en virtut del qual el Responsable utilitza el Servei: el pressupost o el full de comanda acceptats pel Responsable, juntament amb les Condicions de llicència per a centres educatius i organitzacions publicades a https://eco-heroes.org/legal/licence/.
- **«Servei»** significa la plataforma Eco Heroes i el suport descrits a la clàusula 1.1.
- **«Dades del Responsable»** significa les dades personals que l'Encarregat tracta per compte del Responsable en virtut d'aquest Acord, descrites a l'annex I, secció A.
- **«Usuaris»** significa els alumnes, docents, administradors del centre, empleats, personal, hostes i altres persones a qui el Responsable permet utilitzar el Servei.
- **«Subencarregat»** significa un altre encarregat del tractament a qui l'Encarregat recorre per tractar Dades del Responsable.
- **«Dia feiner»** significa de dilluns a divendres, excepte els dies festius a Girona (Espanya).
- Els termes definits a l'article 4 del RGPD, com ara «dades personals», «tractament» i «violació de la seguretat de les dades personals», tenen en aquest Acord el mateix significat.

1. Objecte i durada

1.1 L'Encarregat presta el Servei al Responsable en virtut de la Llicència. El Servei comprèn: el joc d'aventures, el trivial, els jocs de paraules i els qüestionaris de classe en directe; els llibres il·lustrats i la Story Library, els vídeos de les missions, els manuals i els plans de classe; comptes nominatius de docents, gestió de classes i tasques; la importació opcional de llistes de classe (CSV, CSV OneRoster, Google Classroom); l'accés opcional de docents amb Google o Microsoft; la connexió opcional amb la plataforma d'aprenentatge del Responsable mitjançant LTI 1.1 o LTI 1.3; el tauler de classe de l'aplicació mòbil Eco Heroes, quan el Responsable l'utilitzi; els estudis d'impacte opcionals; en les llicències per a empreses i hotels, comptes de coordinador, grups amb codis d'accés per als fills dels treballadors o dels hostes i informes de progrés per grup (CSV), un informe agregat de l'organització, certificats amb el nom de l'organització i inici de sessió opcional del personal amb el proveïdor d'identitat del mateix Responsable; i el suport.

1.2 L'Encarregat tracta les Dades del Responsable durant la vigència de la Llicència i fins que totes les Dades del Responsable s'hagin suprimit o retornat d'acord amb la clàusula 10.

2. Naturalesa i finalitat del tractament; categories

2.1 L'**annex I** recull la naturalesa i la finalitat del tractament, les categories d'interessats i les categories de dades personals.

2.2 L'Encarregat tracta les Dades del Responsable únicament per prestar el Servei al Responsable. No les utilitza per a publicitat, per elaborar perfils de l'alumnat més enllà del progrés d'aprenentatge que el Servei mostra als docents del Responsable, per vendre o cedir dades, ni per desenvolupar cap producte diferent del Servei.

2.3 **Estadístiques anonimitzades.** Quan el Responsable inscriu classes en un estudi d'impacte, instrueix l'Encarregat perquè elabori estadístiques agregades a partir de les respostes, que l'Encarregat pot utilitzar en els seus propis informes i publicacions. L'Encarregat només agrega respostes de grups d'almenys 10 alumnes, no hi inclou mai respostes de text lliure i comprova que no es pugui identificar cap alumne, classe ni centre. Les estadístiques elaborades d'aquesta manera ja no són dades personals. El Responsable pot retirar aquesta instrucció en qualsevol moment mitjançant un

avís per escrit; les respostes recollides a partir de llavors només s'utilitzen per als resultats propis del Responsable.

3. Instruccions

3.1 L'Encarregat tracta les Dades del Responsable únicament seguint instruccions documentades del Responsable, també pel que fa a les transferències a un tercer país o a una organització internacional, llevat que el dret de la Unió o dels estats membres aplicable a l'Encarregat l'obligui a una altra cosa. En aquest cas, l'Encarregat informa el Responsable d'aquesta exigència legal abans del tractament, llevat que aquest dret ho prohibeixi per raons importants d'interès públic.

3.2 Constitueixen instruccions documentades del Responsable aquest Acord, la Llicència i els ajustos que el Responsable i els seus Usuaris triïn al Servei (per exemple, crear classes, importar llistes de classe, activar l'accés únic o la connexió amb una plataforma d'aprenentatge, inscriure una classe en un estudi d'impacte, eliminar alumnes o classes). El contacte administrador del Responsable dona qualsevol altra instrucció per escrit; n'hi ha prou amb un correu electrònic a info@eco-heroes.org.

3.3 L'Encarregat informa immediatament el Responsable si, en la seva opinió, una instrucció infringeix el RGPD, la LOPDGDD o altres disposicions de protecció de dades de la Unió o dels estats membres. L'Encarregat pot suspendre aquesta instrucció fins que el Responsable la confirmi o la modifiqui.

4. Obligacions del Responsable

4.1 El Responsable respon de la licitud del tractament, inclosa la base jurídica per tractar les dades de l'alumnat; de facilitar als interessats la informació que exigeixen els articles 13 i 14 del RGPD (alumnat i, si escau, les seves mares, pares o tutors, docents, administradors, empleats i hostes); d'obtenir el consentiment que exigeixi la llei aplicable al Responsable per a l'alumnat que no hagi assolit l'edat de consentiment digital (article 8 del RGPD; article 7 de la LOPDGDD: 14 anys a Espanya); i de l'exactitud de les dades que ell i els seus Usuaris introdueixin.

4.2 El Responsable indica als seus Usuaris que no introdueixin categories especials de dades personals (article 9 del RGPD), cognoms, adreces de correu electrònic ni altres identificadors directes de l'alumnat en camps de text lliure, com ara àlies, noms de classe, notes de tasques, àlies de qüestionaris en directe i respostes a enquestes.

4.3 Quan el Responsable connecta la seva pròpia plataforma d'aprenentatge (LTI) o el seu proveïdor d'identitat (accés únic), el Responsable respon d'aquest sistema i de configurar-lo perquè comparteixi únicament les dades descrites a l'annex I (en el cas de l'alumnat per LTI, només el nom i mai l'adreça de correu electrònic).

4.4 El Responsable designa un contacte administrador i, abans de dur a terme un estudi d'impacte, un contacte de protecció de la infància, i manté tots dos actualitzats al Servei o mitjançant un correu electrònic a l'Encarregat. Mentre no es designi un contacte de protecció de la infància, o mentre el compte del contacte designat estigui tancat, el Servei trasllada els avisos de protecció de la infància als administradors del centre del Responsable. En les classes que no estan vinculades a cap centre al Servei (per exemple, classes que només es fan servir mitjançant un llançament LTI), els avisos arriben a la persona responsable de protecció de la infància de l'Encarregat, que els trasllada sense demora al contacte administrador del Responsable.

5. Obligacions de l'Encarregat

L'Encarregat:

a. tractarà les Dades del Responsable únicament d'acord amb la clàusula 3;

b. garantirà que tota persona autoritzada per tractar Dades del Responsable estigui subjecta a confidencialitat, per contracte o per llei, i que l'accés als sistemes de producció es limiti a persones identificades que el necessitin;

c. aplicarà les mesures tècniques i organitzatives de l'**annex II** i mantindrà un nivell de seguretat adequat al risc d'acord amb l'article 32 del RGPD, tenint en compte que entre els interessats hi ha menors;

d. recorrerà a un altre encarregat només en els termes de la clàusula 6;

e. tenint en compte la naturalesa del tractament, assistirà el Responsable mitjançant mesures tècniques i organitzatives apropiades, sempre que sigui possible, per respondre a les sol·licituds d'exercici de drets dels interessats (articles 12 a 23 del RGPD), tal com estableix la clàusula 8;

f. ajudarà el Responsable a complir els articles 32 a 36 del RGPD (seguretat, notificació de violacions, avaluació d'impacte relativa a la protecció de dades, consulta prèvia), tenint en compte la naturalesa del tractament i la informació a disposició de l'Encarregat; el resum de l'avaluació d'impacte vigent de l'Encarregat està publicat al Centre de confiança i l'avaluació completa està a disposició del Responsable si la sol·licita;

g. a elecció del Responsable, suprimirà o retornarà totes les Dades del Responsable en acabar el Servei i suprimirà les còpies existents, llevat que el dret de la Unió o dels estats membres n'exigeixi la conservació (clàusula 10);

h. posarà a disposició del Responsable tota la informació necessària per demostrar el compliment de l'article 28 del RGPD, i permetrà i contribuirà a la realització d'auditories, incloses inspeccions, per part del Responsable o d'un auditor que hagi mandatat (clàusula 11);

i. portarà un registre de les categories d'activitats de tractament efectuades per compte del Responsable (article 30.2 del RGPD);

j. transferirà Dades del Responsable a un tercer país només en els termes de la clàusula 7.

6. Subencarregats

6.1 El Responsable atorga una autorització general per escrit per als Subencarregats enumerats a l'**annex III, part A**.

6.2 L'Encarregat informa el Responsable de tota incorporació o substitució prevista d'un Subencarregat amb almenys **30 dies** d'antelació, mitjançant un correu electrònic al contacte administrador del Responsable i actualitzant https://eco-heroes.org/trust/. El Responsable s'hi pot oposar per motius raonables relacionats amb la protecció de dades. Si l'oposició no es pot resoldre dins el termini de preavís, el Responsable pot resoldre la part afectada de la Llicència sense penalització, i s'aplica la clàusula 10.

6.3 L'Encarregat recorre a cada Subencarregat d'acord amb les condicions estàndard de tractament de dades d'aquest proveïdor. Aquestes condicions obliguen el Subencarregat a complir obligacions de protecció de dades que ofereixen garanties suficients de mesures tècniques i organitzatives apropiades, tal com exigeix l'article 28.4 del RGPD. L'Encarregat continua sent plenament responsable davant el Responsable del compliment d'aquestes obligacions per part de cada Subencarregat.

6.4 L'**annex III, part B** enumera serveis de tercers que l'Encarregat utilitza però que **no** tracten Dades del Responsable. No tracten dades personals, o només tracten dades de les quals l'Encarregat és responsable. S'enumeren per transparència i no són Subencarregats als efectes d'aquest Acord.

6.5 Els sistemes propis del Responsable, com ara la seva plataforma d'aprenentatge o el seu entorn de Google o Microsoft, els tria i els controla el Responsable. No són Subencarregats de l'Encarregat.

7. Transferències internacionals

7.1 Les Dades del Responsable s'allotgen i s'emmagatzemen a la Unió Europea: els servidors d'aplicació, a França (Internet Girona, sobre infraestructura d'OVHcloud); la base de dades, les còpies de seguretat xifrades i un servidor de reserva, a Alemanya i Finlàndia (Hetzner Online GmbH). La xarxa de distribució de continguts (Cloudflare) serveix pàgines públiques en memòria cau des de la seva xarxa mundial. Les respostes que contenen dades personals es marquen com a privades i no emmagatzemables (no-store), i la xarxa no les desa en memòria cau.

7.2 L'Encarregat no transfereix Dades del Responsable fora de l'Espai Econòmic Europeu, ni permet que un Subencarregat ho faci, llevat que (i) la destinació compti amb una decisió d'adequació de la Comissió Europea, incloses Suïssa i, per a les organitzacions la certificació de les quals l'Encarregat hagi comprovat a la llista oficial, el Marc de Privacitat de Dades UE-EUA; o (ii) sobre la base de les clàusules contractuals tipus adoptades per la Decisió d'execució (UE) 2021/914 de la Comissió (mòdul 3, d'encarregat a encarregat, o mòdul 2 quan escaigui), amb mesures addicionals quan una avaluació de la transferència mostri que són necessàries. L'annex III indica la garantia aplicable a cada Subencarregat. L'Encarregat manté per escrit una avaluació de la transferència per a cada Subencarregat situat fora de l'EEE i la posa a disposició del Responsable si la sol·licita.

7.3 Cloudflare, Inc. acaba la connexió xifrada a la seva xarxa perimetral, de manera que hi tracta dades de la sol·licitud (adreça IP, adreça sol·licitada, capçaleres). L'Encarregat es basa en les condicions estàndard de tractament de dades de Cloudflare amb les clàusules contractuals tipus i, quan Cloudflare figuri a la llista oficial del Marc de Privacitat de Dades, en el Marc de Privacitat de Dades UE-EUA.

7.4 Proton AG allotja el correu electrònic de l'Encarregat a Suïssa. Suïssa compta amb una decisió d'adequació de la Comissió Europea.

8. Assistència en l'exercici de drets

8.1 Els docents poden consultar, exportar (CSV), canviar el nom, restablir i eliminar les dades d'un alumne, i eliminar classes senceres, directament al Servei. Cada docent veu només les seves pròpies classes; els administradors del centre veuen totes les classes del seu centre i poden retirar immediatament l'accés d'un docent. El Responsable utilitza aquestes funcions per atendre les sol·licituds sempre que pugui.

8.2 Quan una sol·licitud no es pugui atendre mitjançant el Servei, l'Encarregat assisteix el Responsable en un termini de **10 dies feiners** des d'una sol·licitud per escrit. Si l'Encarregat rep directament d'un interessat (incloses mares, pares o tutors) una sol·licitud relativa a Dades del Responsable, no la resol pel que fa al fons. Adreça l'interessat al Responsable sense dilació indeguda i n'informa el Responsable, llevat que aquest li indiqui una altra cosa.

9. Violació de la seguretat de les dades personals

9.1 L'Encarregat notifica al Responsable tota violació de la seguretat de les dades personals que afecti Dades del Responsable sense dilació indeguda i, com a molt tard, en un termini de **48 hores** des que en tingui coneixement. La primera notificació conté la informació que exigeix l'article 33.3 del RGPD en la mesura que es conegui en aquell moment: la naturalesa de la violació, les categories i el nombre aproximat d'interessats i de registres afectats, les conseqüències probables i les mesures adoptades o proposades. L'Encarregat completa la informació per fases a mesura que en disposi.

9.2 L'Encarregat col·labora amb el Responsable per investigar, contenir i documentar la violació, i l'ajuda en qualsevol notificació a l'autoritat de control (a Espanya, l'Agencia Española de Protección de Datos) i en qualsevol comunicació als interessats. L'Encarregat documenta tota violació de la seguretat de les dades personals, inclosos els fets, els seus efectes i les mesures adoptades.

9.3 L'Encarregat envia les notificacions per correu electrònic al contacte administrador del Responsable. Qualsevol persona pot comunicar una vulnerabilitat de seguretat a security@eco-heroes.org. Se n'acusa recepció en un termini de 5 dies feiners i els problemes crítics es corregeixen abans que qualsevol altra feina.

10. Conservació, supressió i retorn

10.1 **Durant la Llicència.** Les Dades del Responsable es conserven d'acord amb el calendari de l'annex I, secció C, que reflecteix les regles de conservació aplicades al codi del Servei. Un docent pot eliminar un alumne o una classe en qualsevol moment, amb efecte immediat a la base de dades activa i a la rèplica de reserva.

10.2 **Exportació.** Durant la Llicència, i fins a la supressió d'acord amb la clàusula 10.3, el Responsable pot exportar al Servei les dades de classe i de progrés en format CSV, o demanar a l'Encarregat una exportació en un format estructurat, d'ús comú i de lectura mecànica.

10.3 **Fi de la Llicència.** Si la Llicència acaba i no es renova, l'Encarregat suprimeix les Dades del Responsable **90 dies** després de la data de finalització. Si el Responsable ho sol·licita per escrit, l'Encarregat suprimeix les Dades del Responsable en un termini de **30 dies** des de la sol·licitud, tant si la Llicència ha acabat com si no. L'Encarregat confirma la supressió per escrit si se li sol·licita. Abans de la supressió, l'Encarregat envia un correu electrònic als administradors del centre del Responsable 30 dies i 7 dies abans de la data de supressió, en què indica aquesta data i com renovar la Llicència o exportar les dades; la supressió no es produeix abans que hagin transcorregut 30 dies des del primer missatge i 7 dies des del segon.

10.4 **Comptes de docents.** Quan acaba l'última llicència vinculada a un compte de docent, el compte continua com a compte gratuït de docent. Se suprimeix 12 mesos després de la finalització d'aquesta llicència, llevat que mentrestant el docent es vinculi a una nova llicència; un compte gratuït se suprimeix després de 12 mesos sense iniciar sessió. L'Encarregat envia un correu electrònic al docent 30 dies abans de la supressió. Mantenir un compte de docent no conserva cap Dada del Responsable: aquestes dades se suprimeixen d'acord amb la clàusula 10.3.

10.5 **Còpies de seguretat i rèplica.** Les dades suprimides desapareixen de les còpies de seguretat en el cicle ordinari. Les còpies de seguretat xifrades es conserven de manera rotatòria, de manera que les dades suprimides desapareixen de totes en un termini de **14 dies**. La rèplica de només lectura del servidor de reserva segueix cada supressió de manera contínua. Les còpies de seguretat només es restauren per recuperar-se d'una pèrdua del sistema de producció; si una restauració recupera dades suprimides, la supressió s'aplica de nou.

10.6 **Conservació legal.** L'Encarregat conserva dades personals després de la fi de la Llicència només quan i durant el temps que ho exigeixi el dret de la Unió o dels estats membres, per exemple les factures i els registres comptables durant 6 anys d'acord amb l'article 30 del Codi de comerç. Aquests registres identifiquen les persones de contacte del Responsable i no contenen dades de l'alumnat. L'Encarregat els protegeix d'acord amb l'annex II i no els utilitza per a cap altra finalitat.

11. Auditoria i informació

11.1 Si se li sol·licita, i com a màxim una vegada per any contractual (o, a més, després d'una violació de la seguretat de les dades personals o davant una sospita documentada i raonable d'incompliment), l'Encarregat facilita al Responsable la informació necessària per demostrar el compliment d'aquest Acord. Inclou el resum de seguretat vigent (https://eco-heroes.org/trust/#security), la llista vigent de Subencarregats, el registre dels tractaments efectuats per compte del Responsable, les avaluacions de les transferències, l'avaluació d'impacte relativa a la protecció de dades, els últims resultats de les proves de restauració i dels assajos de commutació per error i els resultats de qualsevol revisió de seguretat.

11.2 Si aquesta informació no és suficient, el Responsable, o un auditor independent que hagi mandatat i que estigui subjecte a confidencialitat, pot auditar els tractaments pertinents de l'Encarregat amb un preavís d'almenys **30 dies**, en horari laboral i sense pertorbar de manera irraonable les operacions de l'Encarregat ni altres clients. Cada part assumeix els seus propis costos. L'Encarregat pot demanar a l'auditor que signi un compromís de confidencialitat raonable i pot limitar l'accés a sistemes compartits amb altres clients al que sigui necessari per verificar el compliment.

12. Responsabilitat

12.1 Cada part respon davant els interessats d'acord amb l'article 82 del RGPD. Entre les parts, la responsabilitat es regeix per la clàusula de responsabilitat de la Llicència. Res d'aquest Acord ni de la Llicència limita la responsabilitat d'una part quan la llei no permet limitar-la, inclosa la responsabilitat per dol.

12.2 Si l'Encarregat ha de pagar una multa administrativa o una indemnització a causa de les instruccions del Responsable o perquè el Responsable no ha complert les seves obligacions de la clàusula 4, el Responsable manté indemne l'Encarregat en la mesura d'aquesta causa, i el mateix s'aplica a la inversa.

13. Vigència, llei aplicable i jurisdicció

13.1 Aquest Acord entra en vigor en la data d'inici de la Llicència i acaba quan totes les Dades del Responsable s'han suprimit o retornat d'acord amb la clàusula 10. Les clàusules 5(b), 10, 11 i 12 continuen aplicant-se durant el temps necessari.

13.2 Aquest Acord es regeix pel dret espanyol i pel dret de la Unió Europea, inclosos el RGPD i la LOPDGDD. Són competents els jutjats i tribunals de Girona (Espanya), sens perjudici de les normes imperatives aplicables al Responsable com a entitat pública o en virtut de la normativa de contractació pública, i sens perjudici dels drets dels interessats d'acord amb l'article 79 del RGPD. L'annex V afegeix les regles per a responsables al Regne Unit i als Estats Units.

13.3 Les modificacions d'aquest Acord s'han de fer per escrit; n'hi ha prou amb el correu electrònic. L'Encarregat publica el model vigent a https://eco-heroes.org/trust/. Una nova versió del model no modifica un Acord signat llevat que el Responsable ho accepti. L'administrador del centre del

Responsable pot acceptar aquest Acord en línia; l'Encarregat registra qui l'ha acceptat, quan, quina versió i un hash amb clau de l'adreça IP utilitzada.

Signatures

Pel Responsable	Per l'Encarregat — Eco Heroes International SL
Nom, càrrec Data, signatura	Karim Zouhdi, fundador Data, signatura

Annex I — Detalls del tractament

A. Tractament per compte del Responsable (àmbit d'aquest Acord)

Annex I.A — tractament per compte del Responsable

Element	Descripció
Objecte	Prestació del Servei als Usuaris del Responsable en virtut de la Llicència.
Naturalesa	Allotjament, emmagatzematge, visualització i supressió de dades; seguiment del progrés; qüestionaris de classe en directe; tasques; certificats; gestió de classes; importació opcional de llistes de classe facilitades pel Responsable (enganxat o càrrega de CSV, CSV OneRoster 1.1/1.2, Google Classroom); accessos opcionals LTI 1.1 / LTI 1.3 des de la plataforma d'aprenentatge del Responsable, amb aprovisionament de noms i rols (importació de llistes) i serveis de tasques i qualificacions (enviament de puntuacions); accés opcional de docents amb Google o Microsoft triat pel Responsable; el tauler de classe de l'aplicació mòbil Eco Heroes quan el Responsable reparteix un codi de classe; qüestionaris opcionals d'estudis d'impacte a les classes que inscrigui el Responsable; comptes de coordinador, codis d'accés de grup i informes de progrés per grup (CSV) en les llicències per a empreses i hotels; suport. En les llicències d'empresa i d'hotel, a més: informes d'activitat agregats per a l'organització (informe de l'organització i totals, amb qualsevol xifra basada en menys de 5 famílies amagada) i una classificació per equips opcional; el nom i el logotip de l'organització als certificats dels infants; inici de sessió opcional del personal amb el proveïdor d'identitat del mateix Responsable (OpenID Connect).
Finalitat	Impartir educació per a la sostenibilitat basada en els Objectius de Desenvolupament Sostenible de l'ONU, amb la vista de progrés, els informes i l'avaluació que inclou la Llicència. En els estudis d'impacte: l'avaluació per part del Responsable del seu ensenyament (resultats de classe per als seus docents) i estadístiques agregades i anonimitzades d'acord amb la clàusula 2.3. Cap altra finalitat.
Categories d'interessats	Alumnat (el joc està pensat per a edats de 9 a 17 anys en dues franges, 9-12 i 13-17; els plans de classe imprimibles abasten les franges 6–10, 11–13 i 14–17 anys, i el Responsable pot utilitzar el Servei amb alumnat més jove sota la seva pròpia valoració); docents; administradors del centre; mares, pares i tutors, només quan s'utilitzi el procediment de consentiment; en les llicències per a empreses i hotels, els fills dels treballadors o dels hostes i els coordinadors de l'organització.
Dades personals — alumnat (lloc web, en una classe)	Nom o àlies escrit per l'alumne o introduït pel docent (de 2 a 24 caràcters; en les importacions de llistes, el nom de pila més la inicial, ampliada com a màxim a les 3 primeres lletres del cognom només per distingir dos alumnes amb el mateix nom, mai el cognom complet); franja d'edat triada al joc (9-12 o 13-17); avatar d'un conjunt fix; idioma; progrés (punts, objectius i missions completats, estrelles del trivial, nombre de preguntes respostes i encertades per tema); tasques completades; data d'alta i d'última activitat; un identificador aleatori de classe desat al dispositiu de l'alumne per poder desar el progrés. En un qüestionari de classe en directe: l'àlies introduït, les respostes, els temps de resposta i la puntuació. No es recullen: adreça de correu electrònic, cognoms, fotografia, data de naixement, adreça postal, ubicació, identificadors del dispositiu ni publicitaris.

Element	Descripció
Dades personals — alumnat (accessos LTI)	Un hash amb clau de l'identificador d'usuari de la plataforma (per associar un alumne a una plaça); l'identificador d'usuari de la plataforma al registre d'accés durant 90 dies, només quan la plataforma hagi concedit el servei de qualificacions (necessari per enviar la puntuació); nom de pila més la inicial del cognom com a àlies; identificador i títol del curs; rols; configuració regional; última puntuació enviada. No s'emmagatzema cap adreça de correu electrònic ni cap nom complet; el Responsable configura la seva plataforma perquè comparteixi només el nom.
Dades personals — alumnat (aplicació mòbil, tauler de classe)	Activitat (joc diari jugat, data, idioma, punts, finalització, durada; objectius assolits, insígnies) i un hash unidireccional d'un identificador aleatori d'instal·lació generat per l'aplicació. L'alumnat apareix davant el docent amb un àlies generat. El tauler no mostra res en una classe amb menys de cinc alumnes actius.
Dades personals — alumnat (estudi d'impacte, quan el Responsable inscriu una classe)	Respostes al qüestionari de l'estudi (opcions, valoracions i respostes breus opcionals de text lliure), versió del qüestionari, idioma, franja d'edat, hora d'inici i d'enviament i indicadors de qualitat. Les adreces de correu electrònic i els números de telèfon s'eliminen del text lliure en rebre'l. Les respostes que puguin contenir una revelació rellevant per a la protecció de la infància se senyalen al contacte de protecció de la infància designat pel Responsable. Les respostes es vinculen entre les rondes de l'estudi mitjançant un hash unidireccional amb clau de la plaça de l'alumne a la classe; no es recull nom, adreça de correu electrònic ni data de naixement. Per a cada plaça, l'exclusió o el consentiment per escrit que registri el Responsable. Si no s'ha designat cap contacte de protecció de la infància, els destinataris previstos a la clàusula 4.4 n'ocupen el lloc.
Dades personals — docents i administradors del centre	Nom, adreça de correu electrònic professional, centre, rol (docent o administrador del centre), idioma; contrasenya (hash bcrypt) o identificador d'accés únic; secret de verificació en dos passos i codis de reserva en hash si s'ha activat (obligatòria per als administradors del centre); estat de verificació del correu electrònic; hores i nombre d'inicis de sessió; sessions; classes creades; previsualitzacions d'importacions de llistes (només noms, desades a la sessió durant 30 minuts); entrades del registre d'auditoria d'accions administratives (amb un hash amb clau de l'adreça IP i el país de la connexió en codi de 2 lletres, facilitat per la xarxa de distribució de continguts); correspondència de suport.
Dades personals — docents (estudi d'impacte)	Respostes al qüestionari docent i, per a alumnat de 6 a 8 anys, el full d'observació de la classe, vinculades mitjançant un hash unidireccional amb clau del compte o el codi del docent; la inscripció de la classe, la seva modalitat de consentiment i la seva assignació a un grup de l'estudi.
Dades personals — mares, pares i tutors	Només quan s'utilitzi el procediment de consentiment parental del lloc web per a un alumne que no hagi assolit l'edat de consentiment digital: un hash unidireccional amb clau de l'adreça de correu electrònic del progenitor (l'adreça s'utilitza una sola vegada per enviar l'enllaç de confirmació i no s'emmagatzema), la decisió i les marques de temps corresponents.

Element	Descripció
Dades personals — infants i coordinadors (llicències per a empreses i hotels)	Fills dels treballadors o dels hostes del Responsable: s'uneixen a un grup amb el codi d'accés del Responsable i un nom d'heroi (àlies) al seu propi dispositiu o al d'algú de la família, sense compte i sense adreça electrònica. El Servei desa les mateixes dades que per a l'alumnat d'una classe: nom d'heroi, franja d'edat, avatar, idioma, progrés i resultats dels qüestionaris. Coordinadors: nom, adreça electrònica de feina, contrasenya en hash o identificador d'accés, configuració de la verificació en dos passos i els grups que obren. El coordinador veu els objectius completats i els resultats dels qüestionaris per grup i els pot exportar en CSV. Per a l'informe de l'organització, el Servei registra a més per a cada perfil d'heroi d'aquests grups els dies d'activitat i el dia en què es va completar per primera vegada cada objectiu o missió (amb precisió de dia; les classes de les escoles no es registren així). Els informes contenen només dades agregades: cap nom, sobrenom, identificador ni fila per infant; qualsevol xifra basada en 1 a 4 famílies s'amaga (k = 5), i s'amaga una segona xifra quan una de sola permetria deduir-la. Els noms dels equips els tria l'administrador del Responsable i no han d'anomenar persones. Quan el Responsable activa l'inici de sessió d'empresa, els noms i els correus del personal provenen del proveïdor d'identitat del mateix Responsable (àmbits openid, email i profile); aquest proveïdor d'identitat és un sistema i un encarregat del mateix Responsable, no un Subencarregat, i el seu identificador de subjecte es desa només com a hash amb clau. Marca compartida: el nom visible i el logotip de l'organització, facilitats pel Responsable. La pàgina pública de la insígnia que una mare, un pare o un tutor pot compartir a LinkedIn no conté dades personals (un nombre d'objectius, el nom de l'organització si el Responsable ho ha activat i un idioma, tot pres del seu enllaç); la persona adulta inicia l'enviament i l'Encarregat no envia res a LinkedIn.
Categories especials (article 9 del RGPD)	No se sol·liciten ni són necessàries. Vegeu la clàusula 4.2.
Freqüència	Contínua, durant la vigència de la Llicència.

B. Tractaments dels quals Eco Heroes és responsable independent (fora d'aquest Acord)

S'enumeren perquè el Responsable vegi on acaba aquest Acord. Es regeixen per la Política de privacitat (v4.3) i l'Avís de privacitat infantil (v2.2) de l'Encarregat, no per aquest Acord:

- **Els comptes de docents en si:** accés, seguretat, verificació en dos passos i recursos gratuïts per a docents. L'Encarregat és responsable del compte en si i el suprimeix segons la clàusula 10.4; l'activitat del compte per al Responsable són Dades del Responsable.
- **Comptes gratuïts de docents:** docents no vinculats a una llicència que utilitzen els recursos gratuïts per a docents amb una adreça de correu electrònic verificada.
- **Subscripcions familiars** contractades al lloc web per una mare, un pare o un tutor: l'adreça de correu electrònic (desada parcialment emmascarada), les referències de pagament i de subscripció de Stripe i un codi d'accés personal (desat com a hash amb clau). Les dades de la targeta no arriben mai a l'Encarregat. Un codi familiar utilitzat al centre no porta dades del centre.
- **Comptes de l'aplicació** (accés de mares i pares amb Google o Apple; subscripcions a través de Google Play o Apple; estat de la subscripció a través de RevenueCat).
- **Visitants del lloc web** a les pàgines públiques per a adults (Google Analytics 4 després del consentiment; el formulari de contacte a través de Formspree; les sol·licituds de pressupost i d'ambaixadors a través del servidor propi de l'Encarregat; els correus de Dinner Questions a través de Brevo).

- **Classificació pública del trivial** (voluntària: un àlies triat d'una llista generada, la puntuació i un hash amb clau de l'adreça IP; es conserva 30 dies).
- **Enquestes del programa** que l'Encarregat fa fora d'una classe, amb el consentiment de la mare, el pare o el tutor quan la llei ho exigeixi.
- **Serveis diferents:** Eco Heroes Academy (learn.eco-heroes.org) i l'avaluació VSME (assessment.eco-heroes.org) tenen les seves pròpies condicions i informacions de privacitat.

C. Calendari de conservació (tal com s'aplica al Servei)

Annex I.C — calendari de conservació

Dades	Conservació	Mecanisme
Dades de l'alumnat i dels infants de grups d'empreses i hotels (àlies, franja d'edat, avatar, progrés, tasques, activitat de classe a l'aplicació, associació de places LTI)	Durant la Llicència: fins que un docent o administrador elimini l'alumne o la classe. Després de la fi de la Llicència: supressió 90 dies després de la data de finalització, llevat de renovació de la Llicència. A sol·licitud escrita del Responsable: supressió en un termini de 30 dies; els administradors del centre reben un avís per correu electrònic 30 i 7 dies abans de la supressió	Acció del docent o administrador al Servei; supressió automàtica a la fi de la llicència; l'Encarregat a sol·licitud escrita
Dates d'activitat dels perfils d'heroi en grups d'empresa i d'hotel (informe de l'organització)	Es conserven amb el perfil d'heroi i s'eliminen amb ell, segons la regla anterior	Eliminació amb el perfil
Configuració de l'organització: noms d'equips i equip de cada grup, activació de la classificació per equips, nom i logotip de la marca compartida, configuració de l'inici de sessió d'empresa	Durant la vigència de la Llicència; s'elimina a petició del Responsable	Encarregat, a petició
Inici de sessió d'empresa: registres del procés d'inici de sessió; vincles d'identitat fixats (hash amb clau del subjecte del proveïdor d'identitat)	Registres del procés: s'eliminen en fer-se servir o al cap de 10 minuts. Vincles d'identitat: fins que s'elimini el compte o s'elimini o es restableixi la configuració d'inici de sessió del Responsable	Purga automàtica; acció de l'administrador
Qüestionaris de classe en directe (àlies, respostes, temps, puntuacions)	30 dies des de la creació de la sessió del qüestionari	Depuració diària automàtica
Previsualitzacions d'importació de llistes (OneRoster)	30 minuts, només a la sessió del docent al servidor	Caducitat de la sessió
Testimoni d'accés de Google Classroom (importació de llistes)	Només durant la importació, a la sessió del docent; no s'escriu mai a la base de dades	Caducitat de la sessió
Registres d'accessos LTI	Accessos de docents i d'alumnes sense servei de qualificacions: 2 hores. Accessos d'alumnes amb servei de qualificacions: 90 dies	Depuració automàtica amb l'activitat LTI

Dades	Conservació	Mecanisme
Estat d'inici de sessió LTI, testimonis de traspàs, testimonis d'enllaç profund, nonces, testimonis d'importació de llistes	10 minuts / 10 minuts / 60 minuts / 15 minuts / 2 hores	Depuració automàtica; un sol ús
Comptes de docents, de coordinadors i d'administradors del centre	12 mesos després de la fi de l'última llicència vinculada al compte; comptes gratuïts després de 12 mesos sense iniciar sessió; correu d'avís 30 dies abans de la supressió. Registres no verificats: s'eliminen 7 dies després que caduqui l'últim enllaç de confirmació	Depuració automàtica de comptes
Sessions i «recorda'm»	Sessió del servidor durant la seva vida útil configurada, renovada en iniciar sessió i cada 30 minuts; totes les sessions acaben en canviar la contrasenya o quan un administrador retira l'accés. Galeta «recorda'm»: 180 dies (signada amb HMAC)	Codi
Registres de limitació de freqüència (intents d'inici de sessió i altres límits)	30 dies	Depuració diària automàtica
Registre d'auditoria de seguretat (accions administratives, activacions de codis i inicis de sessió; hash amb clau de la IP, país de la connexió en codi de 2 lletres)	12 mesos	Depuració diària automàtica
Hashes d'IP contra abusos en respostes a enquestes i sol·licituds de consentiment	30 dies (la resposta segueix el seu propi termini)	Depuració diària automàtica
Sol·licituds de consentiment parental	Sense resposta o caducades: 30 dies. Denegacions: 12 mesos. Consentiment atorgat: mentre s'invoqui; s'esborra amb les dades en retirar-se el consentiment	Depuració diària automàtica; funció d'esborrat
Respostes d'estudis d'impacte (alumnat, docents, fulls d'observació) i marques d'exclusió o consentiment	24 mesos després del tancament de l'última ronda de l'estudi; abans, per instrucció escrita del Responsable. Les marques d'exclusió i consentiment se suprimeixen amb la inscripció de la classe	Depuració diària automàtica; l'Encarregat a sol·licitud escrita
Avisos de protecció de la infància (respostes d'estudis d'impacte que poden contenir una revelació, amb la plaça i l'àlies als quals pertanyen)	El text de la resposta s'esborra 30 dies després que l'avís es marqui com a atès; el registre de l'avís s'elimina 12 mesos després d'atendre's	Depuració diària automàtica
Respostes a enquestes del programa	24 mesos, o fins que es retiri el consentiment	Depuració diària automàtica; funció d'esborrat

Dades	Conservació	Mecanisme
Entrades de la classificació pública del trivial (fora d'aquest Acord, s'inclouen per completar)	30 dies	Depuració diària automàtica
Registres de l'acceptació d'aquest Acord pel Responsable (qui el va acceptar, quan, quina versió i un hash amb clau de l'adreça IP; els conserva l'Encarregat com a responsable, clàusula 13.3)	Mentre duri la Llicència i 6 anys després que acabi	Registres de l'Encarregat
Registres d'acceptació en el pagament, de cancel·lació i de desistiment dels plans familiars (fora d'aquest Acord, s'inclouen per completar)	6 anys, amb els registres comptables (Codi de comerç, article 30)	Registres comptables
Comptador de taxa de participació derivat d'una persona	2 dies	Depuració diària automàtica
Telemetria (informes d'infraccions de CSP i d'errors de JavaScript)	Sense identificadors emmagatzemats (agent d'usuari escurçat); els comptadors de limitació es reinicien cada minut; registre limitat a 5 MB	Codi
Correspondència de suport (correu electrònic)	Fins que s'atén la sol·licitud, i com a màxim 12 mesos després de l'últim missatge	Procediment de la bústia de l'Encarregat
Còpies de seguretat xifrades	Còpies xifrades conservades de manera rotatòria; les dades suprimides desapareixen de totes les còpies en un termini de 14 dies	Automàtic
Rèplica de la base de dades de reserva	Contínua; segueix cada supressió	Replicació
Registres tècnics del servidor web (adreça IP, adreça sol·licitada)	Fins a 90 dies	Configuració del servidor
Factures i registres de pagament	6 anys (Codi de comerç, article 30); identifiquen les persones de contacte del Responsable, mai l'alumnat	Registres comptables

Annex II — Mesures tècniques i organitzatives (article 32 del RGPD)

Les mesures vigents en la data d'aquest Acord. Es revisen amb cada versió i el resum vigent es publica a https://eco-heroes.org/trust/#security. L'Encarregat pot actualitzar les mesures sempre que el nivell general de seguretat no disminueixi.

1. Xifratge en trànsit

- TLS 1.2 o superior en totes les connexions; HTTP Strict Transport Security amb max-age de dos anys, includeSubDomains i preload; renovació automàtica de certificats; certificats d'origen entre la xarxa de distribució de continguts i els servidors.
- Els servidors d'aplicació es connecten a la base de dades només mitjançant TLS 1.2/1.3, amb verificació del certificat davant una autoritat de certificació fixada; la base de dades rebutja les connexions sense xifrar (require_secure_transport). Els comptes de la base de dades es limiten als equips d'aplicació i de reserva.
- Les còpies de seguretat es xifren (AES-256-CBC, PBKDF2 amb 200 000 iteracions) abans de sortir del servidor i només viatgen per connexions xifrades. No s'escriu cap arxiu sense xifrar.

2. Protecció al navegador

- Content-Security-Policy: els scripts en línia només s'executen si estan aprovats mitjançant un hash SHA-256 per script o mitjançant un nonce per sol·licitud en unes poques pàgines dinàmiques (sense unsafe-inline per a scripts — els estils en línia continuen permesos; object-src 'none', base-uri 'self', frame-ancestors 'none' excepte a les pàgines LTI, que només poden incrustar les plataformes d'aprenentatge registrades). Es recullen els informes d'infraccions, amb limitació de freqüència. Les pàgines pensades per a infants no carreguen scripts de tercers. A les pàgines per a adults, els únics scripts de tercers són Google Analytics, després del consentiment, i la verificació Cloudflare Turnstile als formularis d'accés i de registre.
- Les fonts web s'allotgen al servidor propi de l'Encarregat. No s'envia cap sol·licitud a Google Fonts ni a cap altre proveïdor de fonts.
- Capçaleres de seguretat: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy i Cross-Origin-Resource-Policy same-origin. S'eliminen les capçaleres de versió del servidor i de PHP. Es rebutgen HTTP TRACE i TRACK.
- Galetes: la galeta de sessió és Secure, HttpOnly i SameSite=Strict, amb mode de sessió estricte; l'identificador de sessió canvia en iniciar sessió, en activar un codi i cada 30 minuts. La galeta «recorda'm» està signada amb HMAC amb una clau del servidor. La galeta d'estat LTI es limita a /lti/ i està particionada.
- El service worker dels jocs no desa mai en memòria cau respostes marcades com a no-store o private, ni cap ruta reservada a membres, de manera que no queda contingut de membres a la memòria cau d'un dispositiu compartit després de tancar la sessió.
- Les respostes que contenen dades personals o contingut reservat a membres s'envien amb Cache-Control: private, no-store, i la xarxa de distribució de continguts no les desa mai en memòria cau.

3. Control d'accés i autenticació

- Comptes nominatius de docents: un codi de centre s'utilitza una sola vegada, per donar-se d'alta. Crea un compte nominatiu amb una adreça electrònica verificada o vincula el centre al compte que el docent ja té. Després, el docent hi accedeix amb el seu propi correu i contrasenya, o mitjançant inici de sessió

únic. Un dispositiu que només ha introduït un codi de centre pot jugar, però no té eines docents. Un codi d'administració només dona d'alta el primer compte d'administració del centre i queda esgotat quan aquest compte es confirma; a partir d'aleshores, el professorat s'hi uneix amb un codi de personal que un administrador del centre crea al Servei, que es mostra una sola vegada, es desa només com a hash amb clau i es pot substituir en qualsevol moment.

- Les contrasenyes dels docents es desen amb hash bcrypti es comparen en temps constant. L'adreça de correu electrònic s'ha de verificar abans del primer inici de sessió. Canviar la contrasenya tanca totes les sessions. Un administrador del centre pot retirar immediatament l'accés d'un docent.
- La verificació en dos passos (TOTP, amb codis de reserva en hash) és obligatòria per als administradors del centre i per als superadministradors de l'Encarregat, i qualsevol docent o coordinador d'una llicència d'empresa o d'hotel la pot activar. El codi QR d'alta es genera al servidor, de manera que el secret no en surt mai. El segon factor es comprova abans de crear cap sessió, i els administradors del centre l'han d'utilitzar allà on es veuen dades de l'alumnat. El contacte de protecció de la infància també l'ha d'utilitzar per llegir els avisos de protecció. Després de 10 codis erronis en 24 hores, el segon factor del compte es bloqueja durant 15 minuts i s'avisa per correu electrònic el titular del compte.
- Els codis d'accés es desen només com a hashes amb clau en un fitxer fora de l'arrel web; la clau es desa fora de l'arrel web. Els codis de registre i de llicència es desen de la mateixa manera; un codi es mostra una sola vegada, quan es crea.
- Limitació de freqüència a l'inici de sessió (per adreça IP i per parell correu electrònic/IP, amb un límit global), al registre, al bescanvi de codis, a la incorporació a classes, a la incorporació a qüestionaris en directe, a la sincronització del progrés, al formulari de pressupost, als inicis de sessió LTI, als punts de telemetria i a les consultes de retorn de Stripe. Testimonis CSRF a tot formulari que modifiqui dades. Protecció contra redireccions obertes a tot paràmetre next=.
- Drets d'accés comprovats al servidor: els recursos reservats a membres (vídeos de les missions, bancs de preguntes del trivial, llibres, contingut LTI) només es lliuren després de comprovar al servidor una sessió de codi vàlida, un codi recordat signat o un compte amb sessió iniciada. Res del que el navegador escrigui per si mateix concedeix accés.
- Aïllament per rols i per centre: cada docent veu només les seves pròpies classes; els administradors del centre veuen totes les classes del seu propi centre i res d'altres centres; els docents que accedeixen per LTI veuen només les classes del curs des del qual han accedit; l'accés de superadministrador es limita al personal identificat de l'Encarregat.
- Totes les consultes a la base de dades utilitzen sentències preparades; sense exec, eval ni unserialize; els camins de fitxer es construeixen només a partir d'elements d'una llista permesa; les càrregues (fitxers CSV/ZIP de llistes de classe, imatges d'enquestes) tenen la mida limitada, se'n comprova el tipus i es desen fora de l'arrel web; la visualització d'errors de PHP està desactivada.
- Inici de sessió únic opcional per al personal d'empreses i hotels mitjançant OpenID Connect (Authorization Code amb PKCE; tokens d'identitat signats i verificats en emissor, audiència, caducitat i nonce). Els secrets de client es desen xifrats. Els comptes només s'associen dins dels dominis de correu autoritzats del Responsable i no es vinculen mai a un compte d'una altra organització.

4. Minimització de dades i dades de menors

- No es recullen adreces de correu electrònic, cognoms, fotografies, dates de naixement, adreces postals, ubicacions ni identificadors del dispositiu o publicitaris de l'alumnat. Les importacions de llistes conserven el nom de pila i, com a màxim, les 3 primeres lletres del cognom. L'alumnat per LTI es desa

amb un hash amb clau de l'identificador d'usuari de la plataforma, amb nom de pila i inicial; el Responsable configura la seva plataforma perquè comparteixi només el nom.

- Les adreces IP es desen només com a hashes amb clau (prefix). Qui tingui la clau les podria tornar a vincular, de manera que estan pseudonimitzades, no anonimitzades. Quan acompanyen un contingut, s'eliminen al cap de 30 dies.
- Les pàgines pensades per a infants (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books i les seves versions en altres idiomes) no carreguen analítica ni mostren bàner de consentiment. A les altres pàgines, l'analítica només es carrega després del consentiment exprés.
- Els vídeos de les missions per a membres els allotja l'Encarregat i se serveixen després de la comprovació de drets d'accés. On queda un reproductor de YouTube (joc lliure), utilitza youtube-nocookie.com i només es carrega quan l'usuari prem reproduir.
- Publicar a la classificació pública del trivial és voluntari després de cada partida, amb un àlies generat (un adjectiu i un animal; sense text lliure ni nom de centre). La classificació pública mostra l'àlies i la puntuació dels 10 millors dels últims 30 dies, i les entrades se suprimeixen als 30 dies. Cada fila pública té un enllaç per denunciar-la; una fila denunciada tres vegades s'amaga fins que es revisa. Les classificacions de classe només les veuen el docent d'aquella classe i els administradors del centre, que en poden retirar files.
- Les respostes de text lliure es filtren automàticament en enviar-se: s'eliminen les adreces electròniques i els números de telèfon, i les respostes que coincideixen amb una llista breu de paraules que poden indicar que un infant està en risc es treuen de les dades de l'estudi i es traslladen només a la persona de contacte per a la protecció de la infància designada pel centre. Els noms no s'eliminen automàticament; els investigadors que llegeixen les respostes marquen els possibles noms i mai no els inclouen en cap informe. Una possible revelació es trasllada a la persona de contacte designada pel centre en un termini d'un dia lectiu. Si no s'ha designat cap contacte de protecció de la infància, els destinataris previstos a la clàusula 4.4 n'ocupen el lloc.
- Les adreces de correu electrònic de mares i pares en el procediment de consentiment no es desen mai en clar; només se'n conserva un hash amb clau.
- Els informes de l'organització són agregats: una xifra basada en menys de 5 famílies s'amaga dins del mateix càlcul, de manera que ni la pantalla ni el CSV no la poden mostrar. Només els administradors de l'organització, amb inici de sessió en dos passos, els poden obrir; cada consulta i cada exportació tenen un límit de freqüència i queden registrades.

5. Disponibilitat, còpies de seguretat i recuperació

- El que segueix s'executa automàticament. Un monitor independent (UptimeRobot, 11 monitors, cada 5 minuts) avisa l'Encarregat si alguna cosa falla.
- Una còpia de seguretat xifrada cada nit de la base de dades i de l'aplicació; una còpia es guarda en un centre de dades independent en un altre país de la UE. Cada mes es prova automàticament una restauració.
- Una còpia de seguretat abans de cada versió, amb un procediment de tornada enrere provat; es conserva la versió de producció anterior.
- Un servidor de reserva manté una còpia de l'aplicació i una rèplica en directe de la base de dades. Si falla el servidor web principal, un balanceig de càrrega amb comprovacions d'estat desvia el trànsit automàticament; si falla el servidor de base de dades, la rèplica es promou mitjançant un procediment automatitzat i assajat. Tots dos es van provar l'octubre de 2026.

- Una comprovació horària de la infraestructura (estat i retard de la rèplica, caducitat de certificats, espai en disc, actualitzacions de seguretat pendents, intervals d'adreces de la xarxa de distribució de continguts). Les actualitzacions de seguretat del sistema operatiu s'instal·len automàticament. Protecció contra DDoS i bots al perímetre de la xarxa.
- L'entorn de proves està separat de producció (usuari Unix diferent, pool de PHP amb open_basedir, instància de base de dades diferent, secrets eliminats).

6. Registre i supervisió

- Els esdeveniments de seguretat (inicis de sessió fallits, bescanvis de codis, accions administratives, informes d'infraccions de CSP, supressions i depuracions per conservació) es registren amb hashes amb clau de les adreces IP. El registre d'auditoria de seguretat es conserva 12 mesos i els registres de limitació de freqüència 30 dies (annex I, secció C).
- L'estat del servei en directe i cada incidència es publiquen a la pàgina pública d'estat.

7. Mesures organitzatives

- L'accés als sistemes de producció es limita a persones identificades. Tot compte administratiu (allotjament, servidors de base de dades i de còpies de seguretat, xarxa de distribució de continguts i DNS, repositori de codi font, supervisió, correu electrònic) utilitza autenticació de dos factors. L'accés als servidors es fa amb claus SSH. Els tallafocs limiten l'accés a la base de dades i al servidor de reserva als equips propis de l'Encarregat i als intervals d'adreces de la xarxa de distribució de continguts.
- Els canvis es proven automàticament (integració contínua; una versió es rebutja si el codi no la supera), passen primer per l'entorn de proves i es comproven en directe després de cada versió (47 comprovacions en directe). Es fa i es documenta una revisió estàtica de seguretat de l'aplicació (l'última, el 16 d'octubre de 2026).
- Prova de penetració, octubre de 2026: una prova estructurada de caixa blanca i caixa grisa de la plataforma (autenticació, sessions, control d'accés entre centres, pagaments, exposició de fitxers i dades, limitació d'intents i memòria cau perimetral), feta pel propi equip de proves de l'Encarregat. Totes les troballes crítiques, altes i mitjanes es van corregir i es van tornar a provar abans de la publicació. Està prevista una prova de penetració externa a càrrec d'una empresa independent.
- Es publica un canal de comunicació de vulnerabilitats a /.well-known/security.txt. Se n'acusa recepció en un termini de 5 dies feiners i els problemes crítics es corregeixen abans que qualsevol altra feina.
- Un procediment escrit de gestió d'incidents estableix com l'Encarregat detecta, conté i registra una violació de la seguretat de les dades personals i com compleix el termini de notificació de 48 hores de la clàusula 9.
- L'Encarregat porta un registre dels tractaments que efectua per compte de responsables (article 30.2 del RGPD) i una avaluació de la transferència per a cada Subencarregat situat fora de l'EEE.
- Els terminis de conservació es defineixen al codi que els aplica, de manera que el termini publicat i el termini aplicat no poden divergir.
- Els secrets (clau restringida de Stripe, credencials d'accés únic, claus de hash) es desen fora de l'arrel web i no s'inclouen mai al repositori de codi font.

Annex III — Subencarregats i serveis de tercers

El Centre de confiança (https://eco-heroes.org/trust/#subprocessors) mostra les mateixes dues llistes.

Part A — Subencarregats que tracten Dades del Responsable

Annex III.A — subencarregats autoritzats

Subencarregat	Què fa	On	Garantia per a la transferència
Internet Girona, sobre infraestructura d'OVHcloud	Allotjament web	França (UE)	Dins de la UE; condicions estàndard de tractament de dades del proveïdor
Hetzner Online GmbH, Gunzenhausen, Alemanya	Allotjament de la base de dades, servidor de reserva i còpies de seguretat xifrades	Alemanya i Finlàndia (UE)	Dins de la UE; condicions estàndard de tractament de dades de Hetzner
Cloudflare, Inc., San Francisco, EUA	Distribució de continguts, TLS, protecció contra atacs i bots, la verificació Turnstile als formularis d'accés i de registre, i commutació automàtica en cas de fallada	Xarxa perimetral mundial; servidors d'origen a la UE	Condicions estàndard de tractament de dades de Cloudflare amb les clàusules contractuals tipus (2021/914); Marc de Privacitat de Dades UE-EUA quan Cloudflare figuri a la llista
Proton AG, Ginebra, Suïssa	Allotjament del correu electrònic d'info@ i security@eco-heroes.org: correspondència de suport i de protecció de dades amb el personal del Responsable	Suïssa	Decisió d'adequació de la Comissió Europea per a Suïssa; condicions estàndard de tractament de dades de Proton
Google (Google Ireland Ltd / Google LLC) — només accés i importació de Classroom	Només si el Responsable els activa: accés de docents (nom, adreça de correu electrònic, identificador; sense dades de l'alumnat); importació de llistes de Google Classroom (nom i cognom llegits una vegada i desats com a nom de pila més inicial; el testimoni d'accés es queda a la sessió del docent)	UE / EUA	Condicions de Google del mateix Responsable; condicions estàndard de tractament de dades de Google amb les clàusules contractuals tipus; Marc de Privacitat de Dades UE-EUA quan figuri a la llista
Microsoft (Microsoft Ireland Operations Ltd) — només accés	Només si el Responsable l'activa: accés de docents (només identitat; sense dades de l'alumnat)	UE / EUA	Condicions de Microsoft del mateix Responsable; DPA de productes i serveis de Microsoft amb les clàusules contractuals tipus; Marc de Privacitat de Dades UE-EUA quan figuri a la llista

Subencarregat	Què fa	On	Garantia per a la transferència
Google (YouTube, youtube-nocookie.com)	Reproducció de vídeos educatius seleccionats on encara s'utilitza un reproductor de YouTube: mode de privacitat millorada, carregat només quan l'usuari prem reproduir	UE / EUA	Condicions de Google; Marc de Privacitat de Dades UE-EUA quan figuri a la llista
Moodle Pty Ltd (MoodleCloud), Austràlia Occidental	Només si el Responsable utilitza el lloc de cursos d'Eco Heroes eco-heroes.moodlecloud.com en lloc de la seva pròpia plataforma d'aprenentatge: comptes de curs en aquest lloc i el progrés que els jocs hi comuniquen	Allotjament de MoodleCloud a Amazon Web Services	Acord de tractament de dades de MoodleCloud amb les clàusules contractuals tipus (2021/914) per a tota transferència fora de l'EEE

Part B — Serveis de tercers que no tracten Dades del Responsable

S'enumeren per transparència. Quan hi ha dades personals, s'aplica la Política de privacitat de l'Encarregat. El servidor de correu propi de l'Encarregat envia els correus de compte, de verificació i de servei; no és un tercer.

Annex III.B — serveis de tercers fora d'aquest Acord

Servei	Què fa	On	Per què queda fora d'aquest Acord
Stripe	Pagaments amb targeta de les subscripcions familiars al lloc web; l'Encarregat consulta l'estat del pagament i de la subscripció	UE / EUA; condicions de tractament de dades de Stripe amb les clàusules contractuals tipus; Marc de Privacitat de Dades UE-EUA	Els subscriptors familiars són clients propis de l'Encarregat; no s'envien dades del centre a Stripe
Google Analytics 4	Estadístiques de visites a les pàgines públiques per a adults, només després del consentiment; mai a les pàgines pensades per a infants ni a l'àrea docent	UE / EUA; condicions de tractament de dades de Google amb les clàusules contractuals tipus; Marc de Privacitat de Dades UE-EUA	No s'envia cap Dada del Responsable; l'Encarregat és responsable de les seves pròpies estadístiques web
Formspree	Lliura els missatges enviats amb el formulari de contacte general	EUA; condicions estàndard de tractament de dades del proveïdor (clàusules contractuals tipus; Marc de Privacitat de Dades UE-EUA quan figuri a la llista)	Els missatges són correspondència pròpia de l'Encarregat; el Servei no l'utilitza
Brevo	Correus de Dinner Questions per a famílies (amb subscripció; només l'adreça de correu electrònic)	UE	Butlletí per a famílies; el Servei no l'utilitza
RevenueCat	Estat de la subscripció a l'aplicació (només identificador de compte i historial de compres)	EUA; clàusules contractuals tipus	Comptes familiars de l'aplicació; sense dades del centre

Servei	Què fa	On	Per què queda fora d'aquest Acord
Google Play / Apple App Store	Pagaments de subscripció dins l'aplicació, cobrats per la botiga	UE / EUA	Les botigues venen la subscripció com a responsables independents
Google / Apple (accés a l'aplicació)	Accés opcional de mares i pares a l'aplicació (adreça de correu electrònic i identificador d'accés)	UE / EUA; Marc de Privacitat de Dades UE-EUA, clàusules contractuals tipus	Comptes familiars de l'aplicació; sense dades del centre
UptimeRobot	Comprova que les pàgines públiques i el punt d'estat responen	UE / EUA	No tracta dades personals

Annex IV — Dades de menors

Aquest annex completa els annexos I i II per a l'alumnat menor de 18 anys.

1. **Edat de consentiment digital.** Quan la llei aplicable al Responsable exigeixi el consentiment per a serveis de la societat de la informació oferts directament a un infant (article 8 del RGPD), el Responsable l'obté i el registra. L'edat és de 14 anys a Espanya (article 7 de la LOPDGDD), d'entre 13 i 16 anys als altres estats membres de la UE i de 13 anys al Regne Unit; per als centres dels Estats Units, vegeu l'annex V. Quan el Responsable es basi en una altra base jurídica per a l'ús escolar, com ara el compliment d'una missió realitzada en interès públic, no cal consentiment i el Responsable informa l'alumnat i les famílies. El Servei no comprova l'edat. Les seves dues franges d'edat (9-12 i 13-17) només trien el contingut i la versió dels vídeos.
2. **Procediment de consentiment parental al lloc web.** Quan una funció del lloc web necessita el consentiment d'un progenitor per a un infant que no ha assolit l'edat de consentiment digital, el Servei no registra res fins que el progenitor ho confirma mitjançant un enllaç d'un sol ús enviat per correu electrònic. Només es desen un hash amb clau de l'adreça de correu electrònic del progenitor, la decisió i les marques de temps. Les sol·licituds sense resposta se suprimeixen al cap de 30 dies i les denegacions al cap de 12 mesos. Retirar el consentiment esborra les dades recollides amb aquest consentiment.
3. **Pla familiar.** La subscripció familiar la contracta una mare, un pare o un tutor, que és client de l'Encarregat. Al lloc web, el procés de pagament demana al comprador que confirmi que és major d'edat; a l'aplicació, els passos d'accés i de compra són darrere d'una comprovació per a adults (una pregunta aritmètica escrita). Cap de les dues no és una verificació d'identitat o d'edat. Els infants no obren comptes al lloc web. Un infant pot utilitzar un codi familiar sota la responsabilitat del seu progenitor; no s'hi associen dades del centre.
4. **Sense perfils i sense publicitat.** L'Encarregat no mostra publicitat ni utilitza identificadors o SDK publicitaris. No elabora perfils de l'alumnat més enllà de la vista de progrés que veuen els docents del Responsable, no pren decisions automatitzades amb efectes jurídics o d'importància similar i no ven ni comparteix mai dades de l'alumnat amb finalitats publicitàries.
5. **Sense analítica a les pàgines per a infants.** Les pàgines pensades per a infants (el joc d'aventures, el centre de jocs, el trivial, la biblioteca, les pàgines dels objectius, Wordle, les missions i els llibres, en els 13 idiomes) no carreguen analítica, seguiment ni bàner de consentiment. Només utilitzen l'emmagatzematge del navegador estrictament necessari (idioma, progrés al dispositiu, sessió).
6. **Estudis d'impacte.** Quan el Responsable inscriu classes en un estudi d'impacte, l'alumnat respon a classe com a part de l'avaluació que el mateix Responsable fa del seu ensenyament. El Responsable informa les famílies amb antelació i ofereix la possibilitat d'exclusió, o recull el consentiment per escrit quan la seva llei o la seva normativa ho exigeixin; el Servei admet totes dues opcions i exclou les places afectades. L'alumnat pot ometre qualsevol pregunta i se li indica a la primera pantalla. Els docents només veuen resultats de classe, i només quan almenys 10 alumnes han respost abans i després; cap usuari del centre no veu les respostes individuals d'un alumne. Una resposta de text lliure que pugui contenir una revelació rellevant per a la protecció de la infància es trasllada al contacte de protecció de la infància designat pel Responsable, que decideix què cal fer. L'Encarregat només utilitza resultats agregats i anonimitzats d'acord amb la clàusula 2.3, mai text lliure. Una possible revelació es trasllada a la persona de contacte designada en un termini d'un dia lectiu, i només aquesta persona la veu. Si no s'ha designat cap contacte de protecció de la infància, els destinataris previstos a la clàusula 4.4 n'ocupen el lloc.

7. **Sense funcions de comunicació.** El Servei no té xat, missatgeria ni perfils públics de l'alumnat. La classificació pública del trivial és voluntària, només utilitza àlies triats d'una llista generada, no mostra el nom del centre, conserva les entrades 30 dies i té un enllaç de denúncia a cada entrada. Les classificacions de classe només les veuen el docent de la classe i els administradors del centre, i una entrada pública denunciada tres vegades s'amaga fins que es revisa.
8. **Risc residual comunicat al Responsable.** Un company que conegui un codi de classe i l'àlies d'un alumne pot obrir el progrés d'aquest alumne en un altre dispositiu. Els docents poden veure, canviar el nom o eliminar alumnes en qualsevol moment i poden renovar el codi de classe. El Responsable ho té en compte en la seva pròpia avaluació i en la manera de repartir els codis de classe.
9. **Drets de l'alumnat i de les famílies.** Les famílies i l'alumnat exerceixen els seus drets davant el Responsable. Els docents del Responsable poden consultar, exportar, canviar el nom, restablir i eliminar directament les dades d'un alumne. L'Encarregat adreça al Responsable qualsevol sol·licitud que rebi (clàusula 8.2).
10. **Informació per als infants.** L'Encarregat publica un Avís de privacitat infantil amb una part escrita per als infants (part A) i una part per a famílies i centres (part B) a https://eco-heroes.org/legal/children/. El Responsable el pot reutilitzar en la seva pròpia informació a l'alumnat i a les famílies.

Annex V — Responsables al Regne Unit i als Estats Units

1. **Regne Unit.** Quan el Responsable estigui establert al Regne Unit, les referències d'aquest Acord al RGPD s'entenen fetes al UK GDPR i a la Data Protection Act 2018, i l'autoritat de control competent és la Information Commissioner's Office (ICO). Les Dades del Responsable passen del Regne Unit a l'EEE en virtut de la normativa d'adequació del Regne Unit per a l'EEE. Les transferències ulteriors als Estats Units es basen en l'extensió del Regne Unit al Marc de Privacitat de Dades UE-EUA quan el proveïdor estigui certificat, o en l'addenda del Regne Unit de transferència internacional de dades (UK International Data Transfer Addendum) a les clàusules contractuals tipus. L'Encarregat dissenya el Servei tenint en compte l'Age Appropriate Design Code de la ICO; el seu resum de conformitat figura a la secció 11 de la Política de privacitat.
2. **Estats Units — FERPA.** Quan el Responsable sigui un centre o districte escolar dels Estats Units subjecte a la Family Educational Rights and Privacy Act, l'Encarregat actua com a «school official» amb un interès educatiu legítim d'acord amb 34 CFR 99.31(a)(1)(i)(B). L'Encarregat està sota el control directe del Responsable pel que fa a l'ús i la conservació dels expedients educatius, els utilitza només per a les finalitats de la Llicència i no els comunica a ningú més, excepte als Subencarregats d'acord amb la clàusula 6 o quan la llei ho exigeixi.
3. **Estats Units — COPPA.** Per a l'alumnat menor de 13 anys, el Responsable pot consentir en nom de les famílies la recollida de les dades descrites a l'annex I, tal com permeten les orientacions de la Federal Trade Commission, perquè les dades s'utilitzen només per a les finalitats educatives del Responsable i per a cap altra finalitat comercial. El Responsable manté informades les famílies i transmet les seves sol·licituds de revisar o suprimir les dades del seu fill; l'Encarregat les atén d'acord amb la clàusula 8.
4. **Estats Units — supressió i notificació.** La clàusula 10 s'aplica a la supressió a la fi de la Llicència. Quan una llei estatal sobre privacitat de l'alumnat fixi un termini més breu per a la notificació de violacions o la supressió, l'Encarregat el compleix tan bon punt el Responsable li indiqui quina llei s'aplica.

la Llicència.