Dette er en oversættelse, der stilles til rådighed af praktiske hensyn. Den engelske version er den juridisk bindende tekst og har forrang i tilfælde af uoverensstemmelse. English (PDF)

Databehandleraftale

i henhold til artikel 28 i forordning (EU) 2016/679 (GDPR) og artikel 33 i den spanske organiske lov 3/2018 af 5. december om beskyttelse af personoplysninger og sikring af digitale rettigheder (LOPDGDD) — mellem licenstageren (den „Dataansvarlige“) og Eco Heroes International SL („Databehandleren“)

Parter og roller

Dataansvarlig: _____ (navnet på den skole, skolegruppe, uddannelsesmyndighed, virksomhed eller det hotel, der er nævnt i Licensen), med hjemsted i _____, repræsenteret ved _____ (navn, stilling).
Den Dataansvarliges kontakt for databeskyttelse (administratorkontakt eller, hvis udpeget, databeskyttelsesrådgiver): _____.

Databehandler: Eco Heroes International SL, CIF B44915940, med hjemsted i 17003 Girona (Spanien), registreret i Registro Mercantil de Girona, repræsenteret ved Karim Zouhdi, stifter. Kontakt for databeskyttelse: info@eco-heroes.org, +34 690 814 215. Sikkerhedsindberetninger: security@eco-heroes.org (se https://eco-heroes.org/.well-known/security.txt).

Roller. Den Dataansvarlige bestemmer, hvorfor og hvordan den Dataansvarliges Data behandles, og er dataansvarlig for dem. Databehandleren behandler kun den Dataansvarliges Data på vegne af den Dataansvarlige, som databehandler i henhold til artikel 4, nr. 8, i GDPR.

Lærerkonti. Hver lærer har en personlig konto i eget navn. Databehandleren driver selve kontoen (login, sikkerhed, totrinsbekræftelse og de gratis lærermaterialer) som dataansvarlig i henhold til sin privatlivspolitik. Alt, hvad en lærer gør i Tjenesten for den Dataansvarlige, er den Dataansvarliges Data: kontoens rolle og rettigheder i den Dataansvarliges organisation, klasser, elever, fremskridt, lektier, live-quizzer, import af klasselister, start fra læringsplatformen og effektundersøgelser.

Uden for denne Aftale. Bilag I, del B, nævner de behandlinger, som Databehandleren selv er dataansvarlig for. De er omfattet af Databehandlerens privatlivspolitik (https://eco-heroes.org/legal/privacy/), ikke af denne Aftale. Eco Heroes Academy (learn.eco-heroes.org) og VSME-vurderingen (assessment.eco-heroes.org) er særskilte tjenester med egne vilkår og egne oplysninger om privatliv; denne Aftale omfatter dem ikke.

Denne Aftale er en del af Licensen. Hvis Licensen og denne Aftale er i modstrid med hinanden om behandling af personoplysninger, har denne Aftale forrang.

Definitioner

- **„Licensen“**: den aftale, som den Dataansvarlige bruger Tjenesten i henhold til: det tilbud eller den ordre, den Dataansvarlige har accepteret, sammen med licensvilkårene for skoler og organisationer, der er offentliggjort på https://eco-heroes.org/legal/licence/.
- **„Tjenesten“**: Eco Heroes-platformen og supporten som beskrevet i punkt 1.1.
- **„Den Dataansvarliges Data“**: de personoplysninger, som Databehandleren behandler på vegne af den Dataansvarlige i henhold til denne Aftale, som beskrevet i bilag I, del A.
- **„Brugere“**: de elever, lærere, skoleadministratorer, ansatte, medarbejdere, gæster og andre personer, som den Dataansvarlige giver adgang til at bruge Tjenesten.
- **„Underdatabehandler“**: en anden databehandler, som Databehandleren benytter til at behandle den Dataansvarliges Data.
- **„Arbejdsdag“**: mandag til fredag, undtagen helligdage i Girona (Spanien).
- Begreber, der er defineret i artikel 4 i GDPR, såsom „personoplysninger“, „behandling“ og „brud på persondatasikkerheden“, har samme betydning i denne Aftale.

1. Genstand og varighed

1.1 Databehandleren leverer Tjenesten til den Dataansvarlige i henhold til Licensen. Tjenesten omfatter: eventyrspillet, quizzen, ordspillene og live-klassequizzerne; billedbøgerne og Story Library, missionsvideoerne, håndbøgerne og lektionsarkene; lærerkonti i eget navn, klasseadministration og lektier; valgfri import af klasselister (CSV, OneRoster-CSV, Google Classroom); valgfrit login for lærere med Google eller Microsoft; valgfri forbindelse til den Dataansvarliges læringsplatform via LTI 1.1 eller LTI 1.3; klassedashboardet i Eco Heroes-mobilappen, hvor den Dataansvarlige bruger det; valgfrie effektundersøgelser; ved licenser for virksomheder og hoteller koordinatorkonti, grupper med adgangskoder til ansattes eller gæsters børn og fremskridtsrapporter pr. gruppe (CSV), en samlet organisationsrapport, diplomer med organisationens navn og valgfrit log-ind for medarbejdere via den Dataansvarliges egen identitetsudbyder; og support.

1.2 Databehandleren behandler den Dataansvarliges Data i Licensens løbetid, og indtil alle den Dataansvarliges Data er slettet eller returneret i henhold til punkt 10.

2. Behandlingens art og formål; kategorier

2.1 **Bilag I** beskriver behandlingens art og formål, kategorierne af registrerede og kategorierne af personoplysninger.

2.2 Databehandleren behandler kun den Dataansvarliges Data for at levere Tjenesten til den Dataansvarlige. Den bruger dem ikke til reklame, til at opbygge profiler af elever ud over det læringsfremskridt, som Tjenesten viser den Dataansvarliges lærere, til at sælge eller udleje data eller til at udvikle et andet produkt end Tjenesten.

2.3 **Anonymiserede statistikker.** Når den Dataansvarlige tilmelder klasser til en effektundersøgelse, instruerer den Databehandleren i at udarbejde samlede statistikker ud fra svarene, som Databehandleren må bruge i egne rapporter og publikationer. Databehandleren samler kun svar fra grupper på mindst 10 elever, medtager aldrig fritekstsvar og kontrollerer, at ingen elev, klasse eller skole kan identificeres. Statistikker, der udarbejdes på denne måde, er ikke længere personoplysninger. Den Dataansvarlige kan til enhver tid trække denne instruks tilbage ved skriftlig meddelelse; svar, der indsamles derefter, bruges kun til den Dataansvarliges egne resultater.

3. Instrukser

3.1 Databehandleren behandler kun den Dataansvarliges Data efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsler til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret, som Databehandleren er underlagt. I så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsinteresser.

3.2 Den Dataansvarliges dokumenterede instrukser er denne Aftale, Licensen og de indstillinger, som den Dataansvarlige og dennes Brugere vælger i Tjenesten (f.eks. at oprette klasser, importere klasselister, aktivere single sign-on eller en forbindelse til en læringsplatform, tilmelde en klasse til en effektundersøgelse, slette elever eller klasser). Den Dataansvarliges administratorkontakt giver andre instrukser skriftligt; en e-mail til info@eco-heroes.org er tilstrækkelig.

3.3 Databehandleren underretter straks den Dataansvarlige, hvis en instruks efter dens mening er i strid med GDPR, LOPDGDD eller andre databeskyttelsesbestemmelser i EU-retten eller medlemsstaternes nationale ret. Databehandleren kan udsætte udførelsen af instruksen, indtil den Dataansvarlige bekræfter eller ændrer den.

4. Den Dataansvarliges forpligtelser

4.1 Den Dataansvarlige er ansvarlig for, at behandlingen er lovlig, herunder retsgrundlaget for behandlingen af elevernes data; for at give de registrerede de oplysninger, som artikel 13 og 14 i GDPR kræver (elever og, hvor det er relevant, deres forældre eller værger, lærere, administratorer, ansatte og gæster); for at indhente ethvert samtykke, som den ret, der gælder for den Dataansvarlige, kræver for elever under alderen for digitalt samtykke (artikel 8 i GDPR; artikel 7 i LOPDGDD: 14 år i Spanien); og for rigtigheden af de data, som den og dens Brugere indtaster.

4.2 Den Dataansvarlige beder sine Brugere om ikke at indtaste særlige kategorier af personoplysninger (artikel 9 i GDPR), efternavne, e-mailadresser eller andre direkte identifikatorer for elever i fritekstfelter, såsom kaldenavne, klassenavne, lektienoter, kaldenavne i live-quizzer og svar på undersøgelser.

4.3 Når den Dataansvarlige forbinder sin egen læringsplatform (LTI) eller identitetsudbyder (single sign-on), er den ansvarlig for dette system og dets konfiguration, så det kun deler de data, der er beskrevet i bilag I (for elever via LTI kun navnet, aldrig e-mailadressen).

4.4 Den Dataansvarlige udpeger en administratorkontakt og, før den gennemfører en effektundersøgelse, en kontaktperson for børnebeskyttelse og holder begge kontakter opdateret i Tjenesten eller via e-mail til Databehandleren. Indtil der er udpeget en kontaktperson for børnebeskyttelse, eller mens den udpegede persons konto er lukket, sender Tjenesten børnebeskyttelsesmarkeringer til den Dataansvarliges skoleadministratorer. For klasser, der ikke er knyttet til en skole i Tjenesten (for eksempel klasser, der kun bruges via en LTI-start), går markeringerne til Databehandlerens ansvarlige for børnebeskyttelse, som uden ophold giver dem videre til den Dataansvarliges administratorkontakt.

5. Databehandlerens forpligtelser

Databehandleren:

a. behandler kun den Dataansvarliges Data i henhold til punkt 3;

b. sikrer, at de personer, der er autoriseret til at behandle den Dataansvarliges Data, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og at adgangen til produktionssystemer er begrænset til navngivne personer, der har brug for den;

c. træffer de tekniske og organisatoriske foranstaltninger i **bilag II** og opretholder et sikkerhedsniveau, der passer til risikoen, jf. artikel 32 i GDPR, under hensyntagen til, at de registrerede omfatter børn;

d. gør kun brug af en anden databehandler på betingelserne i punkt 6;

e. bistår, under hensyntagen til behandlingens karakter, den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, i det omfang det er muligt, med at opfylde forpligtelsen til at besvare anmodninger om udøvelse af de registreredes rettigheder (artikel 12-23 i GDPR), som fastsat i punkt 8;

f. bistår den Dataansvarlige med at sikre overholdelse af artikel 32-36 i GDPR (sikkerhed, anmeldelse af brud, konsekvensanalyse vedrørende databeskyttelse, forudgående høring) under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren; et resumé af Databehandlerens gældende konsekvensanalyse er offentliggjort i Trust Centre, og den fulde analyse stilles til rådighed for den Dataansvarlige efter anmodning;

g. sletter eller returnerer efter den Dataansvarliges valg alle den Dataansvarliges Data, når Tjenesten ophører, og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret kræver opbevaring af dataene (punkt 10);

h. stiller alle oplysninger, der er nødvendige for at påvise overholdelse af artikel 28 i GDPR, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, som foretages af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige (punkt 11);

i. fører en fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den Dataansvarlige (artikel 30, stk. 2, i GDPR);

j. overfører kun den Dataansvarliges Data til et tredjeland på betingelserne i punkt 7.

6. Underdatabehandlere

6.1 Den Dataansvarlige giver en generel skriftlig godkendelse af de Underdatabehandlere, der er nævnt i **bilag III, del A**.

6.2 Databehandleren underretter den Dataansvarlige om enhver planlagt tilføjelse eller udskiftning af en Underdatabehandler mindst **30 dage** i forvejen, via e-mail til den Dataansvarliges administratorkontakt og ved opdatering af https://eco-heroes.org/trust/. Den Dataansvarlige kan gøre indsigelse af rimelige grunde vedrørende databeskyttelse. Kan indsigelsen ikke løses inden for varslingsperioden, kan den Dataansvarlige opsige den berørte del af Licensen uden bod, og punkt 10 finder anvendelse.

6.3 Databehandleren benytter hver Underdatabehandler i henhold til denne udbyders standardvilkår for databehandling. Disse vilkår pålægger Underdatabehandleren databeskyttelsesforpligtelser, der giver tilstrækkelige garantier for passende tekniske og organisatoriske foranstaltninger, som artikel 28, stk. 4, i GDPR kræver. Databehandleren forbliver fuldt ansvarlig over for den Dataansvarlige for, at hver Underdatabehandler opfylder disse forpligtelser.

6.4 **Bilag III, del B** nævner tredjepartstjenester, som Databehandleren bruger, men som **ikke** behandler den Dataansvarliges Data. De behandler ingen personoplysninger eller kun oplysninger, som Databehandleren selv er dataansvarlig for. De nævnes af hensyn til gennemsigtigheden og er ikke Underdatabehandlere i denne Aftales forstand.

6.5 Den Dataansvarliges egne systemer, såsom dens læringsplatform eller dens Google- eller Microsoft-miljø, vælges og kontrolleres af den Dataansvarlige. De er ikke Databehandlerens Underdatabehandlere.

7. Internationale overførsler

7.1 Den Dataansvarliges Data hostes og opbevares i Den Europæiske Union: applikationsserverne i Frankrig (Internet Girona, på OVHcloud-infrastruktur); databasen, de krypterede sikkerhedskopier og en reserveserver i Tyskland og Finland (Hetzner Online GmbH). Indholdsleveringsnetværket (Cloudflare) leverer cachelagrede offentlige sider fra sit globale netværk. Svar, der indeholder personoplysninger, er markeret som private og ikke-lagerbare (no-store), og netværket cachelagrer dem ikke.

7.2 Databehandleren overfører ikke den Dataansvarliges Data uden for Det Europæiske Økonomiske Samarbejdsområde og tillader ingen Underdatabehandler at gøre det, medmindre (i) der for destinationen foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Europa-Kommissionen, herunder Schweiz og, for organisationer, hvis certificering Databehandleren har kontrolleret på den officielle liste, databeskyttelsesrammen mellem EU og USA; eller (ii) på grundlag af de standardkontraktbestemmelser, der er vedtaget ved Kommissionens gennemførelsesafgørelse (EU) 2021/914 (modul 3, fra databehandler til databehandler, eller i givet fald modul 2), suppleret med supplerende foranstaltninger, når en vurdering af overførslen viser, at de er nødvendige. Bilag III angiver den garanti, der gælder for hver Underdatabehandler. Databehandleren opbevarer en skriftlig vurdering af overførslen for hver Underdatabehandler uden for EØS og stiller den til rådighed for den Dataansvarlige efter anmodning.

7.3 Cloudflare, Inc. afslutter den krypterede forbindelse ved kanten af sit netværk og behandler derfor dér anmodningsdata (IP-adresse, anmodet adresse, headere). Databehandleren støtter sig på Cloudflares standardvilkår for databehandling med standardkontraktbestemmelserne og, hvis Cloudflare står på den officielle liste over databeskyttelsesrammen, på databeskyttelsesrammen mellem EU og USA.

7.4 Proton AG hoster Databehandlerens e-mail i Schweiz. For Schweiz foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Europa-Kommissionen.

8. Bistand med de registreredes rettigheder

8.1 Lærere kan se, eksportere (CSV), omdøbe, nulstille og slette en elevs data og slette hele klasser direkte i Tjenesten. Hver lærer ser kun sine egne klasser; skoleadministratorer ser alle klasser på deres skole og kan straks fjerne en lærers adgang. Den Dataansvarlige bruger disse funktioner til at besvare anmodninger, når det er muligt.

8.2 Kan en anmodning ikke opfyldes via Tjenesten, bistår Databehandleren den Dataansvarlige inden for **10 arbejdsdage** efter en skriftlig anmodning. Modtager Databehandleren direkte fra en registreret (herunder en forælder eller værge) en anmodning om den Dataansvarliges Data, besvarer den ikke anmodningen i sagen. Den henviser uden unødig forsinkelse den registrerede til den Dataansvarlige og underretter den Dataansvarlige, medmindre denne har givet anden instruks.

9. Brud på persondatasikkerheden

9.1 Databehandleren underretter den Dataansvarlige om ethvert brud på persondatasikkerheden, der berører den Dataansvarliges Data, uden unødig forsinkelse og senest **48 timer** efter at være blevet opmærksom på det. Den første underretning indeholder de oplysninger, som artikel 33, stk. 3, i

GDPR kræver, i det omfang de kendes på det tidspunkt: bruddets karakter, kategorierne og det omtrentlige antal berørte registrerede og registreringer, de sandsynlige konsekvenser og de trufne eller foreslåede foranstaltninger. Databehandleren supplerer oplysningerne trinvis, efterhånden som de bliver tilgængelige.

9.2 Databehandleren samarbejder med den Dataansvarlige om at undersøge, inddæmme og dokumentere bruddet og bistår den Dataansvarlige med enhver anmeldelse til tilsynsmyndigheden (i Spanien Agencia Española de Protección de Datos) og enhver underretning af de registrerede. Databehandleren dokumenterer ethvert brud på persondatasikkerheden, herunder de faktiske omstændigheder, virkningerne og de trufne afhjælpende foranstaltninger.

9.3 Databehandleren sender underretninger via e-mail til den Dataansvarliges administratorkontakt. Enhver kan indberette en sikkerhedssårbarhed til security@eco-heroes.org. Indberetninger bekræftes inden for 5 arbejdsdage, og kritiske problemer rettes før alt andet arbejde.

10. Opbevaring, sletning og returnering

10.1 **I Licensens løbetid.** Den Dataansvarliges Data opbevares efter planen i bilag I, del C, som afspejler de opbevaringsregler, der anvendes i Tjenestens kode. En lærer kan til enhver tid slette en elev eller en klasse med øjeblikkelig virkning i den aktive database og i reservereplikaen.

10.2 **Eksport.** I Licensens løbetid og indtil sletningen efter punkt 10.3 kan den Dataansvarlige eksportere klasse- og fremskridtsdata som CSV i Tjenesten eller bede Databehandleren om en eksport i et struktureret, almindeligt anvendt og maskinlæsbart format.

10.3 **Licensens ophør.** Hvis Licensen ophører og ikke fornyes, sletter Databehandleren den Dataansvarliges Data **90 dage** efter ophørsdatoen. Hvis den Dataansvarlige anmoder skriftligt om det, sletter Databehandleren den Dataansvarliges Data inden for **30 dage** efter anmodningen, uanset om Licensen er ophørt. Databehandleren bekræfter sletningen skriftligt efter anmodning. Inden sletningen sender Databehandleren en e-mail til den Dataansvarliges skoleadministratorer 30 dage og 7 dage før sletningsdatoen med denne dato og oplysning om, hvordan Licensen fornyes eller dataene eksporteres; sletningen sker tidligst 30 dage efter den første og 7 dage efter den anden besked.

10.4 **Lærerkonti.** Når den sidste licens, der er knyttet til en lærerkonto, ophører, fortsætter kontoen som en gratis lærerkonto. Den slettes 12 måneder efter, at den licens ophører, medmindre læreren i mellemtiden knyttes til en ny licens; en gratis konto slettes efter 12 måneder uden login. Databehandleren sender læreren en e-mail 30 dage før sletningen. At en lærerkonto fortsætter, betyder ikke, at nogen af den Dataansvarliges Data bevares: de slettes i henhold til punkt 10.3.

10.5 **Sikkerhedskopier og replika.** Slettede data forsvinder fra sikkerhedskopierne i den normale cyklus. De krypterede sikkerhedskopier opbevares på rullende basis, så slettede data forsvinder fra alle sikkerhedskopier inden for **14 dage**. Den skrivebeskyttede replika på reserveserveren følger løbende hver sletning. Sikkerhedskopier gendannes kun for at afhjælpe et tab af produktionssystemet; hvis en gendannelse genskaber slettede data, anvendes sletningen igen.

10.6 **Lovpligtig opbevaring.** Databehandleren opbevarer kun personoplysninger efter Licensens ophør, i det omfang og så længe EU-retten eller medlemsstaternes nationale ret kræver det, f.eks. fakturaer og regnskabsmateriale i 6 år i henhold til artikel 30 i den spanske handelslov (Código de Comercio). Dette materiale identificerer den Dataansvarliges kontaktpersoner og indeholder ingen elevdata. Databehandleren beskytter det i henhold til bilag II og bruger det ikke til andre formål.

11. Revision og oplysninger

11.1 Efter anmodning og højst én gang pr. aftaleår (eller derudover efter et brud på persondatasikkerheden eller ved en dokumenteret, rimelig mistanke om manglende overholdelse) giver Databehandleren den Dataansvarlige de oplysninger, der er nødvendige for at påvise overholdelse af denne Aftale. Det omfatter det gældende sikkerhedsresumé (https://eco-heroes.org/trust/#security), den gældende liste over Underdatabehandlere, fortegnelsen over behandlinger foretaget på vegne af den Dataansvarlige, overførselsvurderingerne, konsekvensanalysen vedrørende databeskyttelse, de seneste resultater af gendannelsestest og omstillingsøvelser og resultaterne af eventuelle sikkerhedsgennemgange.

11.2 Er disse oplysninger ikke tilstrækkelige, kan den Dataansvarlige eller en uafhængig revisor, som den Dataansvarlige har bemyndiget, og som er underlagt tavshedspligt, revidere Databehandlerens relevante behandlinger med mindst **30 dages** varsel, inden for normal arbejdstid og uden urimelig forstyrrelse af Databehandlerens drift eller andre kunder. Hver part bærer sine egne omkostninger. Databehandleren kan bede revisoren om at underskrive en rimelig fortrolighedserklæring og begrænse adgangen til systemer, der deles med andre kunder, til det, der er nødvendigt for at kontrollere overholdelsen.

12. Ansvar

12.1 Hver part er ansvarlig over for de registrerede i henhold til artikel 82 i GDPR. Mellem parterne er ansvaret reguleret af Licensens ansvarsbestemmelse. Intet i denne Aftale eller Licensen begrænser en parts ansvar, hvor loven ikke tillader en begrænsning, herunder ansvar for forsæt.

12.2 Hvis Databehandleren skal betale en administrativ bøde eller erstatning på grund af den Dataansvarliges instrukser, eller fordi den Dataansvarlige ikke har opfyldt sine forpligtelser i henhold til punkt 4, holder den Dataansvarlige Databehandleren skadesløs i det omfang, årsagen rækker, og omvendt.

13. Varighed, lovvalg og værneting

13.1 Denne Aftale træder i kraft på Licensens startdato og ophører, når alle den Dataansvarliges Data er slettet eller returneret i henhold til punkt 10. Punkt 5(b), 10, 11 og 12 gælder fortsat, så længe det er nødvendigt.

13.2 Denne Aftale er underlagt spansk ret og EU-retten, herunder GDPR og LOPDGDD. Domstolene i Girona (Spanien) er kompetente, uden at dette berører præceptive regler, der gælder for den Dataansvarlige som offentlig myndighed eller i henhold til udbudsretten, og uden at det berører de registreredes rettigheder i henhold til artikel 79 i GDPR. Bilag V tilføjer reglerne for dataansvarlige i Det Forenede Kongerige og USA.

13.3 Ændringer af denne Aftale skal ske skriftligt; en e-mail er tilstrækkelig. Databehandleren offentliggør den gældende skabelon på https://eco-heroes.org/trust/. En ny version af skabelonen ændrer ikke en underskrevet Aftale uden den Dataansvarliges samtykke. Den Dataansvarliges skoleadministrator kan acceptere denne Aftale online; Databehandleren registrerer, hvem der accepterede den, hvornår, hvilken version og en nøglebaseret hash af den anvendte IP-adresse.

Underskrifter

For den Dataansvarlige	For Databehandleren — Eco Heroes International SL

Navn, stilling
Dato, underskrift

Karim Zouhdi, stifter
Dato, underskrift

Bilag I — Beskrivelse af behandlingen

A. Behandling på vegne af den Dataansvarlige (omfattet af denne Aftale)

Bilag I.A — behandling på vegne af den Dataansvarlige

Punkt	Beskrivelse
Genstand	Levering af Tjenesten til den Dataansvarliges Brugere i henhold til Licensen.
Art	Hosting, opbevaring, visning og sletning af data; registrering af fremskridt; live-klassequizzer; lektier; certifikater; klasseadministration; valgfri import af klasselister, som den Dataansvarlige leverer (indsæt eller upload CSV, OneRoster-CSV 1.1/1.2, Google Classroom); valgfri LTI 1.1 / LTI 1.3-start fra den Dataansvarliges læringsplatform med Names and Role Provisioning (import af klasselister) og Assignment and Grade Services (tilbagemelding af point); valgfrit login for lærere med Google eller Microsoft efter den Dataansvarliges valg; klassedashboardet i Eco Heroes-mobilappen, når den Dataansvarlige udleverer en klassekode; valgfrie spørgeskemaer til effektundersøgelser i de klasser, den Dataansvarlige tilmelder; koordinatorkonti, gruppeadgangskoder og fremskridtsrapporter pr. gruppe (CSV) ved licenser for virksomheder og hoteller; support. For virksomheds- og hotellicenser desuden: samlet aktivitetsrapportering til organisationen (organisationsrapport og totaler, hvor ethvert tal, der bygger på færre end 5 familier, skjules) og en valgfri holdrangliste; organisationens navn og logo på børnenes diplomer; valgfrit log-ind for medarbejdere via den Dataansvarliges egen identitetsudbyder (OpenID Connect).
Formål	At give undervisning i bæredygtig udvikling baseret på FN's verdensmål for bæredygtig udvikling med den registrering af fremskridt, rapportering og evaluering, som Licensen fastsætter. Ved effektundersøgelser: den Dataansvarliges evaluering af sin egen undervisning (klasseresultater for dens lærere) og samlede, anonymiserede statistikker i henhold til punkt 2.3. Intet andet formål.
Kategorier af registrerede	Elever (spillet er designet til 9-17-årige i to aldersgrupper, 9-12 og 13-17; de printbare lektionsark dækker trinene 6-10, 11-13 og 14-17 år, og den Dataansvarlige kan efter eget skøn bruge Tjenesten med yngre elever); lærere; skoleadministratorer; forældre og værger, kun når samtykkeproceduren bruges; ved licenser for virksomheder og hoteller ansattes eller gæsters børn og organisationens koordinatorer.
Personoplysninger — elever (websted, i en klasse)	Fornavn eller kaldenavn, som eleven eller læreren indtaster (2-24 tegn; fra import af klasselister fornavn og forbogstav, kun udvidet til højst de første 3 bogstaver af efternavnet for at skelne mellem to elever med samme fornavn — aldrig det fulde navn); aldersgruppe valgt i spillet (9-12 eller 13-17); avatar fra et fast sæt; sprog; fremskridt (point, gennemførte mål og missioner, quizstjerner, antal besvarede og rigtigt besvarede spørgsmål pr. emne); gennemførte lektier; dato for tilmelding og seneste aktivitet; et tilfældigt klassetoken, der gemmes på elevens enhed, så fremskridtet kan gemmes. I en live-klassequiz: det indtastede kaldenavn, svar, svartider og point. Indsamles ikke: e-mailadresse, efternavn, foto, fødselsdato, postadresse, placering, enheds- eller reklame-id'er.

Punkt	Beskrivelse
Personoplysninger — elever (LTI-start)	En nøglebaseret hash af platformens bruger-id (for at knytte en elev til en plads); platformens bruger-id i startposten i 90 dage, kun når platformen har givet adgang til karaktertjenesten (nødvendigt for tilbagemelding af point); fornavn og forbogstav i efternavn som kaldenavn; kursus-id og kursustitel; roller; lokalitet; senest indsendte point. Hverken e-mailadresse eller fulde navn gemmes; den Dataansvarlige konfigurerer sin platform til kun at dele navnet.
Personoplysninger — elever (mobilapp, klassedashboard)	Aktivitet (spillet dagligt spil, dato, sprog, point, gennemførelse, varighed; opnåede mål, badges) og en envejs-hash af et tilfældigt installations-id, som appen genererer. Eleverne vises for læreren under et genereret alias. Dashboardet viser intet for en klasse med færre end fem aktive elever.
Personoplysninger — elever (effektundersøgelse, når den Dataansvarlige tilmelder en klasse)	Svar på undersøgelsens spørgeskema (valg, vurderinger og valgfrie korte fritekstsvar), version af spørgeskemaet, sprog, aldersgruppe, start- og indsendelsestidspunkt og kvalitetsmarkører. E-mailadresser og telefonnumre fjernes fra fritekst ved modtagelsen. Svar, der kan indeholde en betroelse, der er relevant for børnebeskyttelse, markeres over for den kontaktperson, den Dataansvarlige har udpeget. Svarene kobles mellem undersøgelsens runder via en nøglebaseret envejs-hash af elevens plads i klassen; der indsamles hverken navn, e-mailadresse eller fødselsdato. For hver plads den indsigelse eller det skriftlige samtykke, som den Dataansvarlige har registreret. Er der ikke udpeget en kontaktperson for børnebeskyttelse, træder de modtagere, der er nævnt i punkt 4.4, i dens sted.
Personoplysninger — lærere og skoleadministratorer	Navn, arbejds-e-mailadresse, skole, rolle (lærer eller skoleadministrator), sprog; adgangskode (bcrypt-hash) eller id til single sign-on; hemmelighed til totrinsbekræftelse og hashede gendannelseskoder, hvis aktiveret (obligatorisk for skoleadministratorer); status for bekræftelse af e-mail; tidspunkter og antal for login; sessioner; oprettede klasser; forhåndsvisninger af import af klasselister (kun navne, opbevaret i sessionen i 30 minutter); poster i revisionsloggen over administrative handlinger (med en nøglebaseret hash af IP-adressen og forbindelsens land som en kode på 2 bogstaver fra indholdsleveringsnetværket); supportkorrespondance.
Personoplysninger — lærere (effektundersøgelse)	Svar på lærerspørgeskemaet og, for elever på 6-8 år, klassens observationsark, koblet via en nøglebaseret envejs-hash af lærerens konto eller kode; klassens tilmelding, dens samtykkeform og dens fordeling til en gruppe i undersøgelsen.
Personoplysninger — forældre og værger	Kun når webstedets procedure for forældresamtykke bruges for en elev under alderen for digitalt samtykke: en nøglebaseret envejs-hash af forælderens e-mailadresse (selve adressen bruges én gang til at sende bekræftelseslinket og gemmes ikke), beslutningen og dens tidsstempler.

Punkt	Beskrivelse
Personoplysninger — børn og koordinatorer (licenser for virksomheder og hoteller)	Børn af den Dataansvarliges ansatte eller gæster: de slutter sig til en gruppe med den Dataansvarliges adgangskode og et heltenavn (kaldenavn) på deres egen enhed eller en familieenhed, uden konto og uden e-mailadresse. Tjenesten gemmer de samme data som for elever i en klasse: heltenavn, aldersgruppe, avatar, sprog, fremskridt og quizresultater. Koordinatorer: navn, arbejds-e-mailadresse, adgangskode-hash eller login-id, indstillinger for totrinsbekræftelse og de grupper, de opretter. Koordinatoren ser gennemførte mål og quizresultater pr. gruppe og kan eksportere dem som CSV. Til organisationsrapporten registrerer Tjenesten også for hver helteprofil i disse grupper dagene med aktivitet og den dag, hvert mål eller hver mission første gang blev gennemført (på dagsniveau; skoleklasser registreres ikke sådan). Rapporter indeholder kun samlede tal: intet navn, kaldenavn, ingen identifikator og ingen linje pr. barn; ethvert tal, der bygger på 1 til 4 familier, skjules (k = 5), og et andet tal skjules, hvor ét tal alene ville afsløre det. Holdnavne vælges af den Dataansvarliges administrator og må ikke nævne personer. Når den Dataansvarlige slår log-ind via organisationen til, kommer medarbejdernes navne og e-mailadresser fra den Dataansvarliges egen identitetsudbyder (scopes openid, email og profile); denne identitetsudbyder er den Dataansvarliges eget system og egen databehandler, ikke en Underdatabehandler, og dens subjekt-identifikator gemmes kun som en nøglebaseret hash. Co-branding: organisationens visningsnavn og logo, som den Dataansvarlige leverer. Den offentlige badgeside, som en forælder eller værge kan dele på LinkedIn, indeholder ingen personoplysninger (et antal mål, organisationens navn, hvis den Dataansvarlige har tilvalgt det, og et sprog, alt sammen taget fra linket); den voksne sætter delingen i gang, og Databehandleren sender intet til LinkedIn.
Særlige kategorier (artikel 9 i GDPR)	Ingen efterspørges eller er nødvendige. Se punkt 4.2.
Hyppighed	Løbende i Licensens løbetid.

B. Behandlinger, som Eco Heroes selvstændigt er dataansvarlig for (uden for denne Aftale)

Nævnt, så den Dataansvarlige kan se, hvor denne Aftale slutter. De er omfattet af Databehandlerens privatlivspolitik (v4.3) og privatlivsmeddelelse for børn (v2.2), ikke af denne Aftale:

- **Lærerkonti som sådan:** login, sikkerhed, totrinsbekræftelse og de gratis lærermaterialer. Databehandleren er dataansvarlig for selve kontoen og sletter den i henhold til punkt 10.4; kontoens aktivitet for den Dataansvarlige er den Dataansvarliges Data.
- **Gratis lærerkonti:** lærere, der ikke er knyttet til en licens, og som bruger de gratis lærermaterialer (håndbogens lektioner og lærervejledningen) med en bekræftet e-mailadresse.
- **Familieabonnementer** på webstedet, tegnet af en forælder eller værge: e-mailadressen (gemt delvist maskeret), Stripes betalings- og abonnementsreferencer og en personlig adgangskode (gemt som en nøglebaseret hash). Kortoplysninger når aldrig frem til Databehandleren. En familiekode, der bruges i skolen, bærer ingen skoledata med sig.
- **App-konti** (forældres login med Google eller Apple; abonnementer via Google Play eller Apple; abonnementsstatus via RevenueCat).
- **Besøgende på webstedet** på offentlige sider for voksne (Google Analytics 4 efter samtykke; kontaktformularen via Formspree; tilbudsanmodninger og ambassadøransøgninger via Databehandlerens egen server; Dinner Questions-e-mails via Brevo).

- **Quizzens offentlige rangliste** (valgfri: et kaldenavn valgt fra en genereret liste, pointtallet og en nøglebaseret hash af IP-adressen; opbevares i 30 dage).
- **Programundersøgelser,** som Databehandleren gennemfører uden for en klasse, med samtykke fra en forælder, hvor loven kræver det.
- **Særskilte tjenester:** Eco Heroes Academy (learn.eco-heroes.org) og VSME-vurderingen (assessment.eco-heroes.org) har egne vilkår og egne oplysninger om privatliv.

C. Opbevaringsplan (som anvendt i Tjenesten)

Bilag I.C — opbevaringsplan

Data	Opbevaring	Mekanisme
Data om elever og om børn i grupper for virksomheder og hoteller (kaldenavn, aldersgruppe, avatar, fremskridt, lektier, klasseaktivitet i appen, LTI-pladstilknytning)	I Licensens løbetid: indtil en lærer eller administrator sletter eleven eller klassen. Efter Licensens ophør: sletning 90 dage efter ophørsdatoen, medmindre Licensen fornyes. Efter skriftlig anmodning fra den Dataansvarlige: sletning inden for 30 dage; skoleadministratorerne får en e-mail 30 og 7 dage før sletningen	Lærerens eller administratorens handling i Tjenesten; automatisk sletning ved licensens ophør; Databehandleren efter skriftlig anmodning
Aktivitetsdatoer for helteprofiler i virksomheds- og hotelgrupper (organisationsrapport)	Gemmes sammen med helteprofilen og slettes med den efter reglen ovenfor	Slettes med profilen
Organisationens indstillinger: holdnavne og gruppernes holdtilknytning, indstillingen af holdranglisten, navn og logo til co-branding, opsætning af log-ind via organisationen	I Licensens løbetid; slettes efter anmodning fra den Dataansvarlige	Databehandleren efter anmodning
Log-ind via organisationen: registreringer af log-ind-forløbet; fastlåste identitetskoblinger (nøglebaseret hash af identitetsudbyderens subjekt)	Registreringer af forløbet: slettes ved brug eller efter 10 minutter. Identitetskoblinger: indtil kontoen slettes, eller den Dataansvarliges opsætning af log-ind fjernes eller nulstilles	Automatisk sletning; handling fra en administrator
Live-klassequizzer (kaldenavne, svar, tider, point)	30 dage efter oprettelsen af quizsessionen	Automatisk daglig oprydning
Forhåndsvisninger af import af klasselister (OneRoster)	30 minutter, kun i lærerens serversession	Sessionens udløb
Adgangstoken til Google Classroom (import af klasselister)	Kun under importen, i lærerens session; skrives aldrig i databasen	Sessionens udløb
LTI-startposter	Lærerstart og elevstart uden karaktertjeneste: 2 timer. Elevstart med karaktertjeneste: 90 dage	Automatisk oprydning ved LTI-aktivitet

Data	Opbevaring	Mekanisme
LTI-loginstatus, overdragelsestokens, deep linking-tokens, nonces, importtokens til klasselister	10 minutter / 10 minutter / 60 minutter / 15 minutter / 2 timer	Automatisk oprydning; engangsbrug
Konti for lærere, koordinatorer og skoleadministratorer	12 måneder efter ophøret af den sidste licens, der er knyttet til kontoen; gratis konti efter 12 måneder uden login; advarselsmail 30 dage før sletningen. Ikke-bekræftede registreringer: slettes 7 dage efter, at det sidste bekræftelseslink er udløbet	Automatisk oprydning af konti
Sessioner og „husk mig“	Serversession i den konfigurerede varighed, fornyet ved login og hvert 30. minut; alle sessioner ophører ved ændring af adgangskode, eller når en administrator fjerner adgangen. Cookien „husk mig“: 180 dage (HMAC-signeret)	Kode
Poster til hastighedsbegrænsning (loginforsøg og andre grænser)	30 dage	Automatisk daglig oprydning
Sikkerhedsrevisionslog (administrative handlinger, kodeaktiveringer og logins; nøglebaseret hash af IP, forbindelsens land som kode på 2 bogstaver)	12 måneder	Automatisk daglig oprydning
IP-hashes mod misbrug ved svar på undersøgelser og anmodninger om samtykke	30 dage (selve svaret følger sin egen frist)	Automatisk daglig oprydning
Anmodninger om forældresamtykke	Ubesvarede eller udløbne: 30 dage. Afslag: 12 måneder. Givet samtykke: så længe det påberåbes; slettes sammen med dataene, hvis samtykket trækkes tilbage	Automatisk daglig oprydning; sletningsfunktion
Svar fra effektundersøgelser (elever, lærere, observationsark) og markeringer af indsigelse eller samtykke	24 måneder efter afslutningen af undersøgelsens sidste runde; tidligere efter skriftlig instruks fra den Dataansvarlige. Markeringer af indsigelse og samtykke slettes sammen med klassens tilmelding	Automatisk daglig oprydning; Databehandleren efter skriftlig anmodning
Børnebeskyttelsesmarkeringer (svar fra effektundersøgelser, der kan indeholde en betroelse, med den plads og det kaldenavn, de hører til)	Svarets tekst slettes 30 dage efter, at markeringen er markeret som håndteret; selve markeringen slettes 12 måneder efter håndteringen	Automatisk daglig oprydning
Svar på programundersøgelser	24 måneder, eller indtil samtykket trækkes tilbage	Automatisk daglig oprydning; sletningsfunktion

Data	Opbevaring	Mekanisme
Poster på quizzens offentlige rangliste (uden for denne Aftale, nævnt for fuldstændighedens skyld)	30 dage	Automatisk daglig oprydning
Registreringer af den Dataansvarliges accept af denne Aftale (hvem, hvornår, hvilken version, nøglebaseret hash af IP-adressen; opbevares af Databehandleren som dataansvarlig, punkt 13.3)	Så længe Licensen løber og 6 år efter, at den er udløbet	Databehandlerens registreringer
Registreringer af accept ved betaling, opsigelser og fortrydelser af familieplaner (uden for denne Aftale, nævnt for fuldstændighedens skyld)	6 år sammen med regnskabsmaterialet (den spanske handelslov, artikel 30)	Regnskabsmateriale
Tæller for deltagelsesprocent afledt af en person	2 dage	Automatisk daglig oprydning
Telemetri (rapporter om CSP-overtrædelser og JavaScript-fejl)	Ingen identifikatorer gemt (afkortet user agent); hastighedstællere nulstilles hvert minut; log begrænset til 5 MB	Kode
Supportkorrespondance (e-mail)	Indtil anmodningen er behandlet, og højst 12 måneder efter den seneste meddelelse	Procedure for Databehandlerens postkasse
Krypterede sikkerhedskopier	Krypterede sikkerhedskopier opbevares på rullende basis; slettede data forsvinder fra alle sikkerhedskopier inden for 14 dage	Automatisk
Databasens reservereplika	Løbende; følger hver sletning	Replikering
Webserverens tekniske logfiler (IP-adresse, anmodet adresse)	Op til 90 dage	Serverkonfiguration
Fakturaer og betalingsdokumentation	6 år (den spanske handelslov, artikel 30); de identificerer den Dataansvarliges kontaktpersoner, aldrig elever	Regnskabsmateriale

Bilag II — Tekniske og organisatoriske foranstaltninger (artikel 32 i GDPR)

De foranstaltninger, der er gældende på datoen for denne Aftale. De gennemgås ved hver udgivelse, og det gældende resumé er offentliggjort på https://eco-heroes.org/trust/#security. Databehandleren kan opdatere foranstaltningerne, forudsat at det samlede sikkerhedsniveau ikke falder.

1. Kryptering under overførsel

- TLS 1.2 eller nyere for alle forbindelser; HTTP Strict Transport Security med en max-age på to år, includeSubDomains og preload; automatisk fornyelse af certifikater; origin-certifikater mellem indholdsleveringsnetværket og serverne.
- Applikationsserverne forbinder kun til databasen via TLS 1.2/1.3 med kontrol af certifikatet mod en fastlåst certifikatudsteder; databasen afviser ukrypterede forbindelser (require_secure_transport). Databasekonti er begrænset til applikations- og reserveværterne.
- Sikkerhedskopier krypteres (AES-256-CBC, PBKDF2 med 200.000 iterationer), før de forlader serveren, og sendes kun over krypterede forbindelser. Der skrives ingen ukrypterede arkiver.

2. Beskyttelse i browseren

- Content-Security-Policy: inline-scripts kører kun, hvis de er godkendt med en SHA-256-hash pr. script, eller på nogle få dynamiske sider med en nonce pr. anmodning (ingen unsafe-inline for scripts — inline-styles er fortsat tilladt; object-src 'none', base-uri 'self', frame-ancestors 'none' undtagen for LTI-siderne, som kun registrerede læringsplatforme må indlejre). Rapporter om overtrædelser indsamles med hastighedsbegrænsning. Sider for børn indlæser ingen tredjepartsscripts. På sider for voksne er de eneste tredjepartsscripts Google Analytics efter samtykke og Cloudflare Turnstile-kontrollen på login- og registreringsformularer.
- Webskrifttyper hostes på Databehandlerens egen server. Der sendes ingen anmodninger til Google Fonts eller andre udbydere af skrifttyper.
- Sikkerhedsheadere: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy og Cross-Origin-Resource-Policy same-origin. Versionsheadere for server og PHP fjernes. HTTP TRACE og TRACK afvises.
- Cookies: sessionscookien er Secure, HttpOnly og SameSite=Strict, i streng sessionstilstand; sessions-id'et skifter ved login, ved aktivering af en kode og hvert 30. minut. Cookien „husk mig“ er HMAC-signeret med en nøgle på serversiden. LTI-statuscookien er begrænset til /lti/ og partitioneret.
- Spillenes service worker cachelagrer aldrig svar, der er markeret no-store eller private, eller stier kun for medlemmer, så intet beskyttet indhold bliver liggende i cachen på en delt enhed efter logout.
- Svar, der indeholder personoplysninger eller indhold kun for medlemmer, sendes med Cache-Control: private, no-store, og indholdsleveringsnetværket cachelagrer dem aldrig.

3. Adgangskontrol og autentificering

- Lærerkonti i eget navn: en skolekode bruges kun én gang, til tilmelding. Den opretter en konto i eget navn med en bekræftet e-mailadresse eller knytter skolen til lærerens eksisterende konto. Derefter logger læreren ind med egen e-mailadresse og adgangskode eller via single sign-on. En enhed, hvor der kun er indtastet en skolekode, kan spille, men har ingen lærerværktøjer. En administratorkode opretter kun skolens første administratorkonto og er brugt op, når denne konto er bekræftet; derefter tilmelder lærere sig med en personalekode, som en skoleadministrator opretter i Tjenesten, som vises én gang, kun gemmes som nøglebaseret hash og til enhver tid kan udskiftes.

- Læreres adgangskoder hashes med bcryptog sammenlignes i konstant tid. E-mailadressen skal være bekræftet før første login. En ændring af adgangskoden afslutter alle sessioner. En skoleadministrator kan straks fjerne en lærers adgang.
- Totrinsbekræftelse (TOTP med hashede gendannelseskoder) er obligatorisk for skoleadministratorer og for Databehandlerens superadministratorer, og enhver lærer og enhver koordinator for en virksomheds- eller hotellicens kan aktivere den. QR-koden til tilmelding genereres på serveren, så hemmeligheden aldrig forlader den. Den anden faktor kontrolleres, før der oprettes en session, og skoleadministratorer skal bruge den overalt, hvor elevdata er synlige. Kontaktpersonen for børnebeskyttelse skal også bruge den for at læse børnebeskyttelsesmarkeringer. Efter 10 forkerte koder inden for 24 timer låses kontoens anden faktor i 15 minutter, og kontoindehaveren får besked på e-mail.
- Adgangskoder gemmes kun som nøglebaserede hashes i en fil uden for webroden; nøglen opbevares uden for webroden. Registrerings- og licenskoder gemmes på samme måde; en kode vises én gang, når den oprettes.
- Hastighedsbegrænsning ved login (pr. IP-adresse og pr. kombination af e-mail og IP, med et samlet loft), registrering, indløsning af koder, tilmelding til en klasse, tilmelding til en live-quiz, synkronisering af fremskridt, tilbudsformularen, LTI-login, telemetri-endepunkter og Stripe-returopslag. CSRF-tokens på alle formularer, der ændrer data. Beskyttelse mod åbne omdirigeringer på alle next=-parametre.
- Adgangsrettigheder kontrolleres på serveren: ressourcer kun for medlemmer (missionsvideoer, quizzens spørgsmålsbanker, bøger, LTI-indhold) leveres først, når serveren har kontrolleret en gyldig kodesession, en signeret husket kode eller en logget ind konto. Intet, browseren selv skriver, giver adgang.
- Adskillelse efter rolle og skole: hver lærer ser kun sine egne klasser; skoleadministratorer ser alle klasser på deres egen skole og intet fra andre skoler; lærere, der kommer via LTI, ser kun klasserne i det kursus, de startede fra; superadministratoradgang er begrænset til navngivne medarbejdere hos Databehandleren.
- Alle databaseforespørgsler bruger prepared statements; ingen exec, eval eller unserialize; filstier bygges kun af elementer på en godkendt liste; uploads (CSV/ZIP-filer med klasselister, billeder til undersøgelser) er størrelsesbegrænsede, typekontrollerede og gemmes uden for webroden; visning af PHP-fejl er slået fra.
- Valgfrit single sign-on for medarbejdere i virksomheder og hoteller via OpenID Connect (Authorization Code med PKCE; signerede ID-tokens kontrolleret for udsteder, modtager, udløb og nonce). Klienthemmeligheder gemmes krypteret. Konti matches kun inden for den Dataansvarliges tilladte e-maildomæner og kobles aldrig til en konto i en anden organisation.

4. Dataminimering og børns data

- Der indsamles ingen e-mailadresser, efternavne, fotos, fødselsdatoer, postadresser, placeringer eller enheds- eller reklame-id'er for elever. Import af klasselister beholder fornavnet og højst de første 3 bogstaver af efternavnet. Elever, der kommer via LTI, gemmes under en nøglebaseret hash af platformens bruger-id med fornavn og forbogstav; den Dataansvarlige konfigurerer sin platform til kun at dele navnet.
- IP-adresser gemmes kun som nøglebaserede hashes (præfiks). Den, der har nøglen, kan knytte dem sammen igen; de er derfor pseudonymiserede, ikke anonyme. Når de ledsager indhold, slettes de efter 30 dage.
- Sider for børn (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books og deres sprogversioner) indlæser ingen analyse og viser intet samtykkebanner. På andre sider indlæses analyse først efter

udtrykkeligt samtykke.

- Missionsvideoer kun for medlemmer hostes af Databehandleren og leveres efter kontrol af adgangsrettighederne. Hvor der stadig er en YouTube-afspiller (frit spil), bruger den youtube-nocookie.com og indlæses først, når brugeren trykker på afspil.
- Det er frivilligt at offentliggøre på quizzens offentlige rangliste efter hvert spil, under et genereret kaldenavn (et tillægsord og et dyr; ingen fritekst, ingen skoleangivelse). Den offentlige rangliste viser kaldenavn og pointtal for top 10 i de seneste 30 dage, og poster slettes efter 30 dage. Hver offentlig række har et link til indberetning; en række, der indberettes tre gange, skjules, indtil den er gennemgået. Klasseranglister er kun synlige for klassens lærer og skolens administratorer, som kan fjerne rækker.
- Fritekstsvar filtreres automatisk, når de sendes: e-mailadresser og telefonnumre fjernes, og svar, der matcher en kort liste over ord, som kan vise, at et barn er i fare, tages ud af undersøgelsens data og gives kun videre til den kontaktperson for børnebeskyttelse, som skolen har udpeget. Navne fjernes ikke automatisk; de forskere, der læser svarene, markerer mulige navne og nævner dem aldrig i en rapport. En mulig betroelse gives videre til skolens udpegede kontaktperson inden for én skoledag. Er der ikke udpeget en kontaktperson for børnebeskyttelse, træder de modtagere, der er nævnt i punkt 4.4, i dens sted.
- Forældres e-mailadresser i samtykkeproceduren gemmes aldrig i klartekst; kun en nøglebaseret hash opbevares.
- Organisationsrapporter er samlede tal: Et tal, der bygger på færre end 5 familier, skjules allerede i beregningen, så hverken skærmen eller CSV-filen kan vise det. Kun organisationens administratorer med totrinsbekræftelse kan åbne dem; hver visning og hver eksport er begrænset i hyppighed og logges.

5. Tilgængelighed, sikkerhedskopiering og gendannelse

- Følgende kører automatisk. Uafhængig overvågning (UptimeRobot, 11 kontroller, hvert 5. minut) advarer Databehandleren ved en fejl.
- Hver nat en krypteret sikkerhedskopi af databasen og applikationen; en kopi opbevares i et separat datacenter i et andet EU-land. Hver måned testes en gendannelse automatisk.
- En sikkerhedskopi før hver udgivelse med en testet procedure for tilbagerulning; den tidligere produktionsversion bevares.
- En reserveserver har en kopi af applikationen og en løbende replika af databasen. Svigter hovedwebserveren, omdirigerer belastningsfordeling med sundhedstjek trafikken automatisk; svigter databaseserveren, forfremmes replikaen efter en scriptet og indøvet procedure. Begge dele blev testet i oktober 2026.
- En kontrol af infrastrukturen hver time (replikaens status og forsinkelse, certifikaternes udløb, diskplads, afventende sikkerhedsopdateringer, indholdsleveringsnetværkets adresseområder). Styresystemets sikkerhedsopdateringer installeres automatisk. Beskyttelse mod DDoS-angreb og bots ved netværkets kant.
- Testmiljøet er adskilt fra produktionen (separat Unix-bruger, PHP-pool med open_basedir, separat databaseinstans, hemmeligheder fjernet).

6. Logning og overvågning

- Sikkerhedshændelser (mislykkede login, indløsning af koder, administrative handlinger, rapporter om CSP-overtrædelser, sletninger og oprydninger efter opbevaringsfrister) logges med nøglebaserede hashes af IP-adresser. Sikkerhedsrevisionsloggen opbevares i 12 måneder og poster til hastighedsbegrænsning i 30 dage (bilag I, del C).

- Tjenestens aktuelle status og hver afbrydelse offentliggøres på den offentlige statusside.

7. Organisatoriske foranstaltninger

- Adgang til produktionssystemer er begrænset til navngivne personer. Alle administrative konti (hosting, database- og backupservere, indholdsleveringsnetværk og DNS, kildekodedepot, overvågning, e-mail) bruger totrinsbekræftelse. Adgang til serverne sker med SSH-nøgler. Firewalls begrænser adgangen til databasen og reserveserveren til Databehandlerens egne værter og indholdsleveringsnetværkets adresseområder.
- Ændringer testes automatisk (kontinuerlig integration; en udgivelse afvises, hvis koden ikke har bestået testene), går først gennem testmiljøet og kontrolleres i produktion efter hver udgivelse (47 live-kontroller). Der gennemføres og dokumenteres en statisk sikkerhedsgennemgang af applikationen (seneste: 16. oktober 2026).
- Penetrationstest, oktober 2026: en struktureret white box- og grey box-test af platformen (autentificering, sessioner, adgangskontrol mellem skoler, betalinger, eksponering af filer og data, hastighedsbegrænsning og edge-cachen), udført af Databehandlerens eget testteam. Alle kritiske, høje og mellemhøje fund blev rettet og testet igen før udgivelsen. En ekstern penetrationstest udført af et uafhængigt firma er planlagt.
- En kanal til indberetning af sårbarheder er offentliggjort på /.well-known/security.txt. Indberetninger bekræftes inden for 5 arbejdsdage, og kritiske problemer rettes før alt andet arbejde.
- En skriftlig procedure for håndtering af hændelser beskriver, hvordan Databehandleren opdager, inddæmmer og registrerer et brud på persondatasikkerheden, og hvordan den overholder fristen på 48 timer for underretning i punkt 9.
- Databehandleren fører en fortegnelse over de behandlinger, den foretager på vegne af dataansvarlige (artikel 30, stk. 2, i GDPR), og en overførselsvurdering for hver Underdatabehandler uden for EØS.
- Opbevaringsfrister er fastsat i den kode, der anvender dem, så den offentliggjorte og den anvendte frist ikke kan afvige fra hinanden.
- Hemmeligheder (begrænset Stripe-nøgle, legitimationsoplysninger til single sign-on, hash-nøgler) opbevares uden for webroden og lægges aldrig i kildekodedepotet.

Bilag III — Underdatabehandlere og tredjepartstjenester

Trust Centre (https://eco-heroes.org/trust/#subprocessors) viser de samme to lister.

Del A — Underdatabehandlere, der behandler den Dataansvarliges Data

Bilag III.A — godkendte underdatabehandlere

Underdatabehandler	Hvad den gør	Hvor	Garanti for overførslen
Internet Girona, på OVHcloud-infrastruktur	Webhosting	Frankrig (EU)	I EU; udbyderens standardvilkår for databehandling
Hetzner Online GmbH, Gunzenhausen, Tyskland	Databasehosting, reserveserver og krypterede sikkerhedskopier	Tyskland og Finland (EU)	I EU; Hetzners standardvilkår for databehandling
Cloudflare, Inc., San Francisco, USA	Indholdslevering, TLS, beskyttelse mod angreb og bots, Turnstile-kontrol på login- og registreringsformularer og automatisk failover	Globalt kantnetværk; originservere i EU	Cloudflares standardvilkår for databehandling med standardkontraktbestemmelserne (2021/914); databeskyttelsesrammen mellem EU og USA, når Cloudflare står på listen
Proton AG, Genève, Schweiz	Hosting af e-mail info@ og security@eco-heroes.org: support- og databeskyttelseskorrespondance med den Dataansvarliges personale	Schweiz	Europa-Kommissionens afgørelse om tilstrækkeligt beskyttelsesniveau for Schweiz; Protons standardvilkår for databehandling
Google (Google Ireland Ltd / Google LLC) — kun login og Classroom-import	Kun hvis den Dataansvarlige aktiverer dem: login for lærere (navn, e-mailadresse, id; ingen elevdata); import af klasselister fra Google Classroom (for- og efternavn læses én gang og gemmes som fornavn og forbogstav; adgangstokenet bliver i lærerens session)	EU / USA	Den Dataansvarliges egne Google-vilkår; Googles standardvilkår for databehandling med standardkontraktbestemmelserne; databeskyttelsesrammen mellem EU og USA, når den står på listen
Microsoft (Microsoft Ireland Operations Ltd) — kun login	Kun hvis den Dataansvarlige aktiverer det: login for lærere (kun identitet; ingen elevdata)	EU / USA	Den Dataansvarliges egne Microsoft-vilkår; Microsoft Products and Services DPA med standardkontraktbestemmelserne; databeskyttelsesrammen mellem EU og USA, når den står på listen

Underdatabehandler	Hvad den gør	Hvor	Garanti for overførslen
Google (YouTube, youtube-nocookie.com)	Afspilning af udvalgte undervisningsvideoer, hvor der stadig bruges en YouTube-afspiller: tilstand med udvidet beskyttelse af privatlivet, indlæses først, når brugeren trykker på afspil	EU / USA	Googles vilkår; databeskyttelsesrammen mellem EU og USA, når den står på listen
Moodle Pty Ltd (MoodleCloud), Western Australia	Kun hvis den Dataansvarlige bruger Eco Heroes-kursussiden eco-heroes.moodlecloud.com i stedet for sin egen læringsplatform: kursuskonti på den side og det fremskridt, som spillene melder dertil	MoodleCloud-hosting på Amazon Web Services	MoodleClouds databehandleraftale med standardkontraktbestemmelserne (2021/914) for enhver overførsel uden for EØS

Del B — Tredjepartstjenester, der ikke behandler den Dataansvarliges Data

Nævnt af hensyn til gennemsigtigheden. Hvor personoplysninger er involveret, gælder Databehandlerens privatlivspolitik. Databehandlerens egen mailserver sender konto-, bekræftelses- og servicemails; den er ikke en tredjepart.

Bilag III.B — tredjepartstjenester uden for denne Aftale

Tjeneste	Hvad den gør	Hvor	Hvorfor den er uden for denne Aftale
Stripe	Kortbetaling af familieabonnementer på webstedet; Databehandleren læser betalings- og abonnementsstatus	EU / USA; Stripes vilkår for databehandling med standardkontraktbestemmelserne; databeskyttelsesrammen mellem EU og USA	Familieabonnenter er Databehandlerens egne kunder; der sendes ingen skoledata til Stripe
Google Analytics 4	Besøgsstatistik på offentlige sider for voksne, kun efter samtykke; aldrig på sider for børn eller i lærerområdet	EU / USA; Googles vilkår for databehandling med standardkontraktbestemmelserne; databeskyttelsesrammen mellem EU og USA	Der sendes ingen af den Dataansvarliges Data; Databehandleren er dataansvarlig for sin egen webstatistik
Formspree	Videresender beskeder fra den generelle kontaktformular	USA; udbyderens standardvilkår for databehandling (standardkontraktbestemmelser; databeskyttelsesrammen mellem EU og USA, når den står på listen)	Beskederne er Databehandlerens egen korrespondance; bruges ikke af Tjenesten
Brevo	Dinner Questions-e-mails til familier (efter tilmelding; kun e-mailadresse)	EU	Nyhedsbrev til familier; bruges ikke af Tjenesten
RevenueCat	Abonnementsstatus i appen (kun konto-id og købshistorik)	USA; standardkontraktbestemmelser	Appens familiekonti; ingen skoledata

Tjeneste	Hvad den gør	Hvor	Hvorfor den er uden for denne Aftale
Google Play / Apple App Store	Abonnementsbetalinger i appen, opkrævet af butikken	EU / USA	Butikkerne sælger abonnementet som selvstændige dataansvarlige
Google / Apple (login i appen)	Valgfrit login for forældre i appen (e-mailadresse og login-id)	EU / USA; databeskyttelsesrammen mellem EU og USA, standardkontraktbestemmelser	Appens familiekonti; ingen skoledata
UptimeRobot	Kontrollerer, at offentlige sider og statusendepunktet svarer	EU / USA	Behandler ingen personoplysninger

Bilag IV — Børns data

Dette bilag supplerer bilag I og II for elever under 18 år.

1. **Alder for digitalt samtykke.** Når den ret, der gælder for den Dataansvarlige, kræver samtykke til informationssamfundstjenester, der tilbydes direkte til et barn (artikel 8 i GDPR), indhenter og registrerer den Dataansvarlige det. Alderen er 14 år i Spanien (artikel 7 i LOPDGDD), 13-16 år i de øvrige EU-medlemsstater og 13 år i Det Forenede Kongerige; for skoler i USA se bilag V. Hvis den Dataansvarlige bygger skolebrugen på et andet retsgrundlag, f.eks. en opgave i samfundets interesse, er samtykke ikke nødvendigt, og den Dataansvarlige oplyser elever og forældre. Tjenesten kontrollerer ikke alder. Dens to aldersgrupper (9-12 og 13-17) vælger kun indhold og videoversion.
2. **Procedure for forældresamtykke på webstedet.** Når en funktion på webstedet kræver samtykke fra en forælder for et barn under alderen for digitalt samtykke, gemmer Tjenesten intet, før forælderen har bekræftet via et engangslink sendt via e-mail. Kun en nøglebaseret hash af forælderens e-mailadresse, beslutningen og tidsstemplerne gemmes. Ubesvarede anmodninger slettes efter 30 dage og afslag efter 12 måneder. Tilbagetrækning af samtykket sletter de data, der er indsamlet på grundlag af det.
3. **Familieplan.** En forælder eller værge tegner familieabonnementet og er Databehandlerens kunde. På webstedet beder betalingen køberen bekræfte at være myndig; i appen ligger login og køb bag en voksenkontrol (et regnestykke, der skal tastes). Ingen af dem er en identitets- eller alderskontrol. Børn opretter ikke konti på webstedet. Et barn kan bruge en familiekode under forælderens ansvar; der er ingen skoledata knyttet til den.
4. **Ingen profilering og ingen reklame.** Databehandleren viser ingen reklamer og bruger ingen reklame-id'er eller reklame-SDK'er. Den opbygger ingen profiler af elever ud over den registrering af fremskridt, som den Dataansvarliges lærere ser, træffer ingen automatiske afgørelser med retsvirkning eller tilsvarende betydelig virkning og sælger eller deler aldrig elevdata til reklame.
5. **Ingen analyse på sider for børn.** Sider for børn (eventyrspillet, spilsamlingen, quizzen, biblioteket, siderne om målene, Wordle, missionerne og bøgerne, på alle 13 sprog) indlæser ingen analyse, ingen trackere og intet samtykkebanner. De bruger kun den strengt nødvendige lagring i browseren (sprog, fremskridt på enheden, session).
6. **Effektundersøgelser.** Når den Dataansvarlige tilmelder klasser til en effektundersøgelse, svarer eleverne i timen som en del af den Dataansvarliges egen evaluering af undervisningen. Den Dataansvarlige oplyser forældrene på forhånd og giver dem mulighed for at gøre indsigelse eller indhenter skriftligt samtykke, hvor dens ret eller regler kræver det; Tjenesten understøtter begge dele og udelukker de berørte pladser. Eleverne kan springe ethvert spørgsmål over og får det at vide på den første skærm. Lærerne ser kun klasseresultater og kun, når mindst 10 elever har svaret før og efter; ingen bruger på skolen ser en elevs individuelle svar. Et fritekstsvar, der kan indeholde en betroelse, der er relevant for børnebeskyttelse, sendes videre til den kontaktperson, den Dataansvarlige har udpeget, som beslutter, hvad der skal ske. Databehandleren bruger kun samlede, anonymiserede resultater i henhold til punkt 2.3, aldrig fritekst. En mulig betroelse gives videre til den udpegede kontaktperson inden for én skoledag, og kun denne kontaktperson ser den. Er der ikke udpeget en kontaktperson for børnebeskyttelse, træder de modtagere, der er nævnt i punkt 4.4, i dens sted.
7. **Ingen kommunikationsfunktioner.** Tjenesten har ingen chat, ingen beskeder og ingen offentlige elevprofiler. Quizzens offentlige rangliste er frivillig, bruger kun kaldenavne fra en genereret liste, viser ingen skolenavne, opbevarer poster i 30 dage og har et link til indberetning ved hver post. Klasseranglister er kun synlige for klassens lærer og skolens administratorer, og en offentlig post, der indberettes tre gange, skjules, indtil den er gennemgået.

8. **Restrisiko meddelt den Dataansvarlige.** En klassekammerat, der kender en klassekode og en elevs kaldenavn, kan åbne elevens fremskridt på en anden enhed. Lærere kan til enhver tid se, omdøbe eller fjerne elever og kan forny klassekoden. Den Dataansvarlige tager højde for dette i sin egen vurdering og i den måde, den udleverer klassekoder på.
9. **Forældres og elevers rettigheder.** Forældre og elever udøver deres rettigheder over for den Dataansvarlige. Den Dataansvarliges lærere kan direkte se, eksportere, omdøbe, nulstille og slette en elevs data. Databehandleren videresender enhver anmodning, den modtager, til den Dataansvarlige (punkt 8.2).
10. **Oplysninger til børn.** Databehandleren offentliggør en privatlivsmeddelelse for børn med en del skrevet til børn (del A) og en del til forældre og skoler (del B) på https://eco-heroes.org/legal/children/. Den Dataansvarlige kan bruge den i sine egne oplysninger til elever og forældre.

Bilag V — Dataansvarlige i Det Forenede Kongerige og USA

1. **Det Forenede Kongerige.** Hvis den Dataansvarlige er etableret i Det Forenede Kongerige, læses denne Aftales henvisninger til GDPR som henvisninger til UK GDPR og Data Protection Act 2018, og den kompetente tilsynsmyndighed er Information Commissioner's Office (ICO). Den Dataansvarliges Data overføres fra Det Forenede Kongerige til EØS i henhold til britiske regler om tilstrækkeligt beskyttelsesniveau for EØS. Videreoverførsler til USA bygger på den britiske udvidelse af databeskyttelsesrammen mellem EU og USA, når udbyderen er certificeret, eller på UK International Data Transfer Addendum til standardkontraktbestemmelserne. Databehandleren udformer Tjenesten med hensyntagen til ICO's Age Appropriate Design Code; dens resumé af overholdelsen står i afsnit 11 i privatlivspolitikken.
2. **USA — FERPA.** Hvis den Dataansvarlige er en skole eller et skoledistrikt i USA, der er omfattet af Family Educational Rights and Privacy Act, handler Databehandleren som „school official“ med en legitim uddannelsesmæssig interesse i henhold til 34 CFR 99.31(a)(1)(i)(B). Databehandleren er under den Dataansvarliges direkte kontrol med hensyn til brug og vedligeholdelse af elevjournaler, bruger dem kun til Licensens formål og videregiver dem ikke til andre, undtagen til Underdatabehandlere i henhold til punkt 6, eller når loven kræver det.
3. **USA — COPPA.** For elever under 13 år kan den Dataansvarlige på forældrenes vegne give samtykke til indsamlingen af de data, der er beskrevet i bilag I, som Federal Trade Commissions vejledning tillader, fordi dataene kun bruges til den Dataansvarliges uddannelsesformål og ikke til andre kommercielle formål. Den Dataansvarlige holder forældrene orienteret og videresender deres anmodninger om at se eller slette deres barns data; Databehandleren efterkommer dem i henhold til punkt 8.
4. **USA — sletning og underretning.** Punkt 10 gælder for sletning ved Licensens ophør. Hvis en delstatslov om elevers privatliv fastsætter en kortere frist for underretning om brud eller for sletning, overholder Databehandleren den, så snart den Dataansvarlige oplyser, hvilken lov der gælder.
