Ceci est une traduction fournie à titre de commodité. La version anglaise constitue le texte juridiquement contraignant et prévaut en cas de divergence. English (PDF)

Accord de sous-traitance

au titre de l'article 28 du règlement (UE) 2016/679 (RGPD) et de l'article 33 de la loi organique espagnole 3/2018 du 5 décembre relative à la protection des données personnelles et à la garantie des droits numériques (LOPDGDD) — entre le titulaire de la licence (le « Responsable du traitement ») et Eco Heroes International SL (le « Sous-traitant »)

Parties et rôles

Responsable du traitement : _____ (nom de l'établissement scolaire, du groupe d'établissements, de l'autorité éducative, de l'entreprise ou de l'hôtel désigné dans la Licence), dont le siège est situé _____, représenté par _____ (nom, fonction).
Contact du Responsable du traitement pour la protection des données (contact administrateur ou, s'il est désigné, délégué à la protection des données) : _____.

Sous-traitant : Eco Heroes International SL, CIF B44915940, dont le siège social est situé 17003 Girona (Espagne), immatriculée au Registro Mercantil de Girona, représentée par Karim Zouhdi, fondateur. Contact pour la protection des données : info@eco-heroes.org, +34 690 814 215. Signalements de sécurité : security@eco-heroes.org (voir https://eco-heroes.org/.well-known/security.txt).

Rôles. Le Responsable du traitement décide pourquoi et comment les Données du Responsable sont traitées et en est le responsable du traitement. Le Sous-traitant traite les Données du Responsable uniquement pour le compte du Responsable du traitement, en qualité de sous-traitant au sens de l'article 4, point 8, du RGPD.

Comptes enseignants. Chaque enseignant dispose d'un compte personnel et nominatif. Le Sous-traitant gère le compte lui-même (connexion, sécurité, authentification à deux facteurs et ressources gratuites pour enseignants) en qualité de responsable du traitement, conformément à sa Politique de confidentialité. Tout ce qu'un enseignant fait dans le Service pour le Responsable du traitement constitue des Données du Responsable : le rôle et les droits du compte dans l'établissement du Responsable du traitement, les classes, les élèves, la progression, les devoirs, les quiz en direct, les importations de listes de classe, les lancements depuis la plateforme d'apprentissage et les études d'impact.

Hors du présent Accord. L'annexe I, section B, énumère les traitements dont le Sous-traitant est lui-même responsable. Ces traitements relèvent de la Politique de confidentialité du Sous-traitant (https://eco-heroes.org/legal/privacy/), et non du présent Accord. Eco Heroes Academy (learn.eco-heroes.org) et l'évaluation VSME (assessment.eco-heroes.org) sont des services distincts, avec leurs propres conditions et informations sur la confidentialité ; le présent Accord ne les couvre pas.

> Le présent Accord fait partie de la Licence. En cas de contradiction entre la Licence et le présent Accord concernant le traitement de données à caractère personnel, le présent Accord prévaut.

Définitions

- **« Licence »** désigne le contrat en vertu duquel le Responsable du traitement utilise le Service : le devis ou le bon de commande accepté par le Responsable du traitement, ainsi que les Conditions de licence pour les établissements et organisations publiées à l'adresse https://eco-heroes.org/legal/licence/.
- **« Service »** désigne la plateforme Eco Heroes et l'assistance décrites à la clause 1.1.
- **« Données du Responsable »** désigne les données à caractère personnel que le Sous-traitant traite pour le compte du Responsable du traitement au titre du présent Accord, décrites à l'annexe I, section A.
- **« Utilisateurs »** désigne les élèves, enseignants, administrateurs d'établissement, salariés, personnels, clients hébergés et autres personnes que le Responsable du traitement autorise à utiliser le Service.
- **« Sous-traitant ultérieur »** désigne un autre sous-traitant auquel le Sous-traitant fait appel pour traiter des Données du Responsable.
- **« Jour ouvré »** désigne du lundi au vendredi, hors jours fériés à Girona (Espagne).
- Les termes définis à l'article 4 du RGPD, tels que « données à caractère personnel », « traitement » et « violation de données à caractère personnel », ont le même sens dans le présent Accord.

1. Objet et durée

1.1 Le Sous-traitant fournit le Service au Responsable du traitement au titre de la Licence. Le Service comprend : le jeu d'aventure, le quiz, les jeux de mots et les quiz de classe en direct ; les livres illustrés et la Story Library, les vidéos des missions, les manuels et les fiches pédagogiques ; les comptes enseignants nominatifs, la gestion des classes et les devoirs ; l'importation facultative de listes de classe (CSV, CSV OneRoster, Google Classroom) ; la connexion facultative des enseignants avec Google ou Microsoft ; la connexion facultative à la plateforme d'apprentissage du Responsable du traitement par LTI 1.1 ou LTI 1.3 ; le tableau de bord de classe de l'application mobile Eco Heroes, lorsque le Responsable du traitement l'utilise ; les études d'impact facultatives ; pour les licences entreprises et hôtels, les comptes de coordinateur, les groupes avec codes d'accès pour les enfants des salariés ou des clients, et les rapports de progression par groupe (CSV), un rapport agrégé de l'organisation, des certificats portant le nom de l'organisation et la connexion facultative du personnel via le fournisseur d'identité du Responsable du traitement ; et l'assistance.

1.2 Le Sous-traitant traite les Données du Responsable pendant la durée de la Licence et jusqu'à ce que toutes les Données du Responsable aient été supprimées ou restituées conformément à la clause 10.

2. Nature et finalité du traitement ; catégories

2.1 L'**annexe I** décrit la nature et la finalité du traitement, les catégories de personnes concernées et les catégories de données à caractère personnel.

2.2 Le Sous-traitant traite les Données du Responsable uniquement pour fournir le Service au Responsable du traitement. Il ne les utilise pas à des fins publicitaires, pour établir des profils d'élèves allant au-delà de la progression d'apprentissage que le Service montre aux enseignants du Responsable du traitement, pour vendre ou louer des données, ni pour développer un produit autre que le Service.

2.3 **Statistiques anonymisées.** Lorsque le Responsable du traitement inscrit des classes à une étude d'impact, il charge le Sous-traitant d'établir des statistiques agrégées à partir des réponses, que le Sous-traitant peut utiliser dans ses propres rapports et publications. Le Sous-traitant n'agrège que des réponses de groupes d'au moins 10 élèves, n'y inclut jamais de réponses en texte libre et vérifie qu'aucun élève, aucune classe ni aucun établissement ne peut être identifié. Les statistiques ainsi établies ne sont plus des données à caractère personnel. Le Responsable du traitement peut retirer cette instruction à tout moment par avis écrit ; les réponses recueillies ensuite ne servent qu'aux résultats propres du Responsable du traitement.

3. Instructions

3.1 Le Sous-traitant ne traite les Données du Responsable que sur instruction documentée du Responsable du traitement, y compris en ce qui concerne les transferts vers un pays tiers ou une organisation internationale, à moins que le droit de l'Union ou d'un État membre auquel le Sous-traitant est soumis ne l'exige. Dans ce cas, le Sous-traitant informe le Responsable du traitement de cette obligation juridique avant le traitement, sauf si ce droit l'interdit pour des motifs importants d'intérêt public.

3.2 Constituent les instructions documentées du Responsable du traitement : le présent Accord, la Licence et les paramètres que le Responsable du traitement et ses Utilisateurs choisissent dans le Service (par exemple créer des classes, importer des listes de classe, activer l'authentification unique ou une connexion à une plateforme d'apprentissage, inscrire une classe à une étude d'impact, supprimer des élèves ou des classes). Le contact administrateur du Responsable du traitement donne toute autre instruction par écrit ; un e-mail à info@eco-heroes.org suffit.

3.3 Le Sous-traitant informe immédiatement le Responsable du traitement si, selon lui, une instruction constitue une violation du RGPD, de la LOPDGDD ou d'autres dispositions du droit de l'Union ou des États membres relatives à la protection des données. Le Sous-traitant peut suspendre l'exécution de cette instruction jusqu'à ce que le Responsable du traitement la confirme ou la modifie.

4. Obligations du Responsable du traitement

4.1 Le Responsable du traitement répond de la licéité du traitement, y compris de la base juridique du traitement des données des élèves ; de la fourniture aux personnes concernées des informations exigées par les articles 13 et 14 du RGPD (élèves et, le cas échéant, leurs parents ou représentants légaux, enseignants, administrateurs, salariés et clients) ; de l'obtention de tout consentement que la loi applicable au Responsable du traitement exige pour les élèves n'ayant pas atteint l'âge du consentement numérique (article 8 du RGPD ; article 7 de la LOPDGDD : 14 ans en Espagne) ; et de l'exactitude des données que lui-même et ses Utilisateurs saisissent.

4.2 Le Responsable du traitement demande à ses Utilisateurs de ne pas saisir de catégories particulières de données à caractère personnel (article 9 du RGPD), de noms de famille, d'adresses e-mail ou d'autres identifiants directs d'élèves dans les champs de texte libre, tels que les pseudonymes, les noms de classe, les notes de devoirs, les pseudonymes des quiz en direct et les réponses aux enquêtes.

4.3 Lorsque le Responsable du traitement connecte sa propre plateforme d'apprentissage (LTI) ou son fournisseur d'identité (authentification unique), il répond de ce système et de sa configuration, afin qu'il ne partage que les données décrites à l'annexe I (pour les élèves via LTI, le nom uniquement et jamais l'adresse e-mail).

4.4 Le Responsable du traitement désigne un contact administrateur et, avant de mener une étude d'impact, un référent en matière de protection de l'enfance, et tient ces deux contacts à jour dans le Service ou par e-mail au Sous-traitant. Tant qu'aucun référent en matière de protection de l'enfance n'est désigné, ou tant que le compte du référent désigné est fermé, le Service transmet les signalements de protection de l'enfance aux administrateurs d'établissement du Responsable du traitement. Pour les classes qui ne sont rattachées à aucun établissement dans le Service (par exemple les classes utilisées uniquement via un lancement LTI), les signalements parviennent au référent protection de l'enfance du Sous-traitant, qui les transmet sans délai au contact administrateur du Responsable du traitement.

5. Obligations du Sous-traitant

Le Sous-traitant :

a. traite les Données du Responsable uniquement conformément à la clause 3 ;

b. veille à ce que toute personne autorisée à traiter des Données du Responsable soit tenue à la confidentialité, par contrat ou par la loi, et à ce que l'accès aux systèmes de production soit limité à des personnes nommément désignées qui en ont besoin ;

c. met en œuvre les mesures techniques et organisationnelles de l'**annexe II** et maintient un niveau de sécurité adapté au risque conformément à l'article 32 du RGPD, compte tenu du fait que les personnes concernées comprennent des enfants ;

d. ne fait appel à un autre sous-traitant que dans les conditions de la clause 6 ;

e. compte tenu de la nature du traitement, aide le Responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à répondre aux demandes d'exercice des droits des personnes concernées (articles 12 à 23 du RGPD), comme le prévoit la clause 8 ;

f. aide le Responsable du traitement à respecter les articles 32 à 36 du RGPD (sécurité, notification des violations, analyse d'impact relative à la protection des données, consultation préalable), compte tenu de la nature du traitement et des informations dont il dispose ; le résumé de l'analyse d'impact en vigueur du Sous-traitant est publié dans le Centre de confiance et l'analyse complète est mise à la disposition du Responsable du traitement sur demande ;

g. selon le choix du Responsable du traitement, supprime ou restitue toutes les Données du Responsable au terme du Service et détruit les copies existantes, à moins que le droit de l'Union ou d'un État membre n'en exige la conservation (clause 10) ;

h. met à la disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect de l'article 28 du RGPD, et permet la réalisation d'audits, y compris d'inspections, par le Responsable du traitement ou un auditeur qu'il a mandaté, et y contribue (clause 11) ;

i. tient un registre des catégories d'activités de traitement effectuées pour le compte du Responsable du traitement (article 30, paragraphe 2, du RGPD) ;

j. ne transfère des Données du Responsable vers un pays tiers que dans les conditions de la clause 7.

6. Sous-traitants ultérieurs

6.1 Le Responsable du traitement donne une autorisation écrite générale pour les Sous-traitants ultérieurs énumérés à l'**annexe III, partie A**.

6.2 Le Sous-traitant informe le Responsable du traitement de tout ajout ou remplacement prévu d'un Sous-traitant ultérieur au moins **30 jours** à l'avance, par e-mail au contact administrateur du Responsable du traitement et par la mise à jour de https://eco-heroes.org/trust/. Le Responsable du

traitement peut s'y opposer pour des motifs raisonnables liés à la protection des données. Si l'objection ne peut être résolue dans le délai de préavis, le Responsable du traitement peut résilier la partie concernée de la Licence sans pénalité, et la clause 10 s'applique.

6.3 Le Sous-traitant fait appel à chaque Sous-traitant ultérieur conformément aux conditions standard de traitement des données de ce fournisseur. Ces conditions imposent au Sous-traitant ultérieur des obligations en matière de protection des données qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, comme l'exige l'article 28, paragraphe 4, du RGPD. Le Sous-traitant demeure pleinement responsable à l'égard du Responsable du traitement de l'exécution de ces obligations par chaque Sous-traitant ultérieur.

6.4 L'**annexe III, partie B** énumère les services tiers que le Sous-traitant utilise mais qui **ne traitent pas** de Données du Responsable. Ils ne traitent aucune donnée à caractère personnel, ou uniquement des données dont le Sous-traitant est lui-même responsable. Ils sont mentionnés par transparence et ne sont pas des Sous-traitants ultérieurs au sens du présent Accord.

6.5 Les systèmes propres du Responsable du traitement, tels que sa plateforme d'apprentissage ou son environnement Google ou Microsoft, sont choisis et contrôlés par le Responsable du traitement. Ils ne sont pas des Sous-traitants ultérieurs du Sous-traitant.

7. Transferts internationaux

7.1 Les Données du Responsable sont hébergées et stockées dans l'Union européenne : les serveurs d'application en France (Internet Girona, sur l'infrastructure d'OVHcloud) ; la base de données, les sauvegardes chiffrées et un serveur de secours en Allemagne et en Finlande (Hetzner Online GmbH). Le réseau de diffusion de contenu (Cloudflare) sert des pages publiques mises en cache depuis son réseau mondial. Les réponses contenant des données à caractère personnel sont marquées comme privées et non stockables (no-store), et le réseau ne les met pas en cache.

7.2 Le Sous-traitant ne transfère pas de Données du Responsable hors de l'Espace économique européen, et n'autorise aucun Sous-traitant ultérieur à le faire, sauf (i) lorsque la destination bénéficie d'une décision d'adéquation de la Commission européenne, y compris la Suisse et, pour les organisations dont le Sous-traitant a vérifié la certification sur la liste officielle, le cadre de protection des données UE–États-Unis ; ou (ii) sur la base des clauses contractuelles types adoptées par la décision d'exécution (UE) 2021/914 de la Commission (module 3, de sous-traitant à sous-traitant, ou module 2 le cas échéant), complétées par des mesures supplémentaires lorsqu'une évaluation du transfert montre qu'elles sont nécessaires. L'annexe III indique la garantie applicable à chaque Sous-traitant ultérieur. Le Sous-traitant conserve par écrit une évaluation du transfert pour chaque Sous-traitant ultérieur situé hors de l'EEE et la met à la disposition du Responsable du traitement sur demande.

7.3 Cloudflare, Inc. termine la connexion chiffrée à la périphérie de son réseau et y traite donc des données de requête (adresse IP, adresse demandée, en-têtes). Le Sous-traitant s'appuie sur les conditions standard de traitement des données de Cloudflare comprenant les clauses contractuelles types et, lorsque Cloudflare figure sur la liste officielle du cadre de protection des données, sur le cadre de protection des données UE–États-Unis.

7.4 Proton AG héberge la messagerie du Sous-traitant en Suisse. La Suisse bénéficie d'une décision d'adéquation de la Commission européenne.

8. Assistance pour l'exercice des droits

8.1 Les enseignants peuvent consulter, exporter (CSV), renommer, réinitialiser et supprimer les données d'un élève, et supprimer des classes entières, directement dans le Service. Chaque enseignant ne voit

que ses propres classes ; les administrateurs d'établissement voient toutes les classes de leur établissement et peuvent retirer immédiatement l'accès d'un enseignant. Le Responsable du traitement utilise ces fonctions pour répondre aux demandes chaque fois qu'il le peut.

8.2 Lorsqu'une demande ne peut être satisfaite au moyen du Service, le Sous-traitant aide le Responsable du traitement dans un délai de **10 jours ouvrés** à compter d'une demande écrite. Si le Sous-traitant reçoit directement d'une personne concernée (y compris d'un parent ou représentant légal) une demande relative à des Données du Responsable, il n'y répond pas sur le fond. Il oriente la personne concernée vers le Responsable du traitement dans les meilleurs délais et en informe le Responsable du traitement, sauf instruction contraire de ce dernier.

9. Violation de données à caractère personnel

9.1 Le Sous-traitant notifie au Responsable du traitement toute violation de données à caractère personnel affectant des Données du Responsable dans les meilleurs délais et au plus tard **48 heures** après en avoir pris connaissance. La première notification contient les informations exigées par l'article 33, paragraphe 3, du RGPD dans la mesure où elles sont connues à ce moment : la nature de la violation, les catégories et le nombre approximatif de personnes concernées et d'enregistrements concernés, les conséquences probables et les mesures prises ou envisagées. Le Sous-traitant complète ces informations de manière échelonnée à mesure qu'elles deviennent disponibles.

9.2 Le Sous-traitant coopère avec le Responsable du traitement pour enquêter sur la violation, la contenir et la documenter, et l'aide pour toute notification à l'autorité de contrôle (en Espagne, l'Agencia Española de Protección de Datos) et pour toute communication aux personnes concernées. Le Sous-traitant documente toute violation de données à caractère personnel, y compris les faits, ses effets et les mesures prises.

9.3 Le Sous-traitant envoie les notifications par e-mail au contact administrateur du Responsable du traitement. Toute personne peut signaler une vulnérabilité de sécurité à security@eco-heroes.org. Les signalements font l'objet d'un accusé de réception dans un délai de 5 jours ouvrés, et les problèmes critiques sont corrigés avant tout autre travail.

10. Conservation, suppression et restitution

10.1 **Pendant la Licence.** Les Données du Responsable sont conservées selon le calendrier de l'annexe I, section C, qui reflète les règles de conservation appliquées dans le code du Service. Un enseignant peut supprimer un élève ou une classe à tout moment, avec effet immédiat dans la base de données active et dans la réplique de secours.

10.2 **Export.** Pendant la Licence, et jusqu'à la suppression prévue à la clause 10.3, le Responsable du traitement peut exporter dans le Service les données de classe et de progression au format CSV, ou demander au Sous-traitant un export dans un format structuré, couramment utilisé et lisible par machine.

10.3 **Fin de la Licence.** Si la Licence prend fin et n'est pas renouvelée, le Sous-traitant supprime les Données du Responsable **90 jours** après la date de fin. Si le Responsable du traitement le demande par écrit, le Sous-traitant supprime les Données du Responsable dans un délai de **30 jours** à compter de la demande, que la Licence ait pris fin ou non. Le Sous-traitant confirme la suppression par écrit sur demande. Avant la suppression, le Sous-traitant envoie un courriel aux administrateurs d'établissement du Responsable du traitement 30 jours et 7 jours avant la date de suppression, en indiquant cette date et la manière de renouveler la Licence ou d'exporter les données ; la suppression n'intervient pas avant 30 jours après le premier message et 7 jours après le second.

10.4 **Comptes enseignants.** Lorsque la dernière licence liée à un compte enseignant prend fin, le compte se poursuit en tant que compte enseignant gratuit. Il est supprimé 12 mois après la fin de cette licence, sauf si l'enseignant est rattaché entre-temps à une nouvelle licence ; un compte gratuit est supprimé après 12 mois sans connexion. Le Sous-traitant envoie un e-mail à l'enseignant 30 jours avant la suppression. Le maintien d'un compte enseignant ne conserve aucune Donnée du Responsable : ces données sont supprimées conformément à la clause 10.3.

10.5 **Sauvegardes et réplique.** Les données supprimées disparaissent des sauvegardes au fil du cycle normal. Les sauvegardes chiffrées sont conservées par rotation, de sorte que les données supprimées disparaissent de toutes les sauvegardes dans un délai de **14 jours**. La réplique en lecture seule du serveur de secours suit chaque suppression en continu. Les sauvegardes ne sont restaurées que pour remédier à une perte du système de production ; si une restauration rétablit des données supprimées, la suppression est appliquée de nouveau.

10.6 **Conservation légale.** Le Sous-traitant ne conserve des données à caractère personnel après la fin de la Licence que dans la mesure et pour la durée exigées par le droit de l'Union ou d'un État membre, par exemple les factures et les documents comptables pendant 6 ans conformément à l'article 30 du code de commerce espagnol (Código de Comercio). Ces documents identifient les personnes de contact du Responsable du traitement et ne contiennent aucune donnée d'élève. Le Sous-traitant les protège conformément à l'annexe II et ne les utilise à aucune autre fin.

11. Audit et information

11.1 Sur demande, et au plus une fois par année contractuelle (ou en outre après une violation de données à caractère personnel ou en cas de soupçon documenté et raisonnable de non-conformité), le Sous-traitant fournit au Responsable du traitement les informations nécessaires pour démontrer le respect du présent Accord. Elles comprennent la synthèse de sécurité en vigueur (https://eco-heroes.org/trust/#security), la liste en vigueur des Sous-traitants ultérieurs, le registre des traitements effectués pour le compte du Responsable du traitement, les évaluations des transferts, l'analyse d'impact relative à la protection des données, les derniers résultats des tests de restauration et des exercices de basculement et les résultats de toute revue de sécurité.

11.2 Si ces informations ne suffisent pas, le Responsable du traitement, ou un auditeur indépendant qu'il a mandaté et qui est tenu à la confidentialité, peut auditer les traitements concernés du Sous-traitant moyennant un préavis d'au moins **30 jours**, pendant les heures ouvrables et sans perturbation déraisonnable des activités du Sous-traitant ou des autres clients. Chaque partie supporte ses propres frais. Le Sous-traitant peut demander à l'auditeur de signer un engagement de confidentialité raisonnable et limiter l'accès aux systèmes partagés avec d'autres clients à ce qui est nécessaire pour vérifier la conformité.

12. Responsabilité

12.1 Chaque partie est responsable envers les personnes concernées conformément à l'article 82 du RGPD. Entre les parties, la responsabilité est régie par la clause de responsabilité de la Licence. Aucune disposition du présent Accord ni de la Licence ne limite la responsabilité d'une partie lorsque la loi ne permet pas de la limiter, y compris la responsabilité pour faute intentionnelle.

12.2 Si le Sous-traitant doit payer une amende administrative ou des dommages-intérêts en raison des instructions du Responsable du traitement ou parce que ce dernier n'a pas respecté ses obligations au titre de la clause 4, le Responsable du traitement garantit le Sous-traitant dans la mesure de cette cause, et réciproquement.

13. Durée, droit applicable et juridiction

13.1 Le présent Accord entre en vigueur à la date de début de la Licence et prend fin lorsque toutes les Données du Responsable ont été supprimées ou restituées conformément à la clause 10. Les clauses 5(b), 10, 11 et 12 continuent de s'appliquer aussi longtemps que nécessaire.

13.2 Le présent Accord est régi par le droit espagnol et le droit de l'Union européenne, y compris le RGPD et la LOPDGDD. Les tribunaux de Girona (Espagne) sont compétents, sans préjudice des règles impératives applicables au Responsable du traitement en tant qu'organisme public ou en vertu du droit des marchés publics, et sans préjudice des droits des personnes concernées au titre de l'article 79 du RGPD. L'annexe V ajoute les règles applicables aux responsables du traitement au Royaume-Uni et aux États-Unis.

13.3 Toute modification du présent Accord doit être faite par écrit ; un e-mail suffit. Le Sous-traitant publie le modèle en vigueur à l'adresse https://eco-heroes.org/trust/. Une nouvelle version du modèle ne modifie pas un Accord signé sans l'accord du Responsable du traitement. L'administrateur d'établissement du Responsable du traitement peut accepter le présent Accord en ligne ; le Sous-traitant enregistre qui l'a accepté, quand, quelle version et un hachage à clé de l'adresse IP utilisée.

Signatures

Pour le Responsable du traitement	Pour le Sous-traitant — Eco Heroes International SL
Nom, fonction	Karim Zouhdi, fondateur
Date, signature	Date, signature

Annexe I — Description du traitement

A. Traitement pour le compte du Responsable du traitement (champ du présent Accord)

Annexe I.A — traitement pour le compte du Responsable du traitement

Élément	Description
Objet	Fourniture du Service aux Utilisateurs du Responsable du traitement au titre de la Licence.
Nature	Hébergement, stockage, affichage et suppression de données ; suivi de la progression ; quiz de classe en direct ; devoirs ; certificats ; gestion des classes ; importation facultative de listes de classe fournies par le Responsable du traitement (collage ou chargement de CSV, CSV OneRoster 1.1/1.2, Google Classroom) ; lancements facultatifs LTI 1.1 / LTI 1.3 depuis la plateforme d'apprentissage du Responsable du traitement, avec provisionnement des noms et rôles (importation de listes) et services de devoirs et de notes (remontée des scores) ; connexion facultative des enseignants avec Google ou Microsoft choisie par le Responsable du traitement ; tableau de bord de classe de l'application mobile Eco Heroes lorsque le Responsable du traitement distribue un code de classe ; questionnaires facultatifs d'études d'impact dans les classes inscrites par le Responsable du traitement ; comptes de coordinateur, codes d'accès de groupe et rapports de progression par groupe (CSV) pour les licences entreprises et hôtels ; assistance. Pour les licences d'entreprise et d'hôtel, également : rapports d'activité agrégés pour l'organisation (rapport de l'organisation et totaux, tout chiffre reposant sur moins de 5 familles étant masqué) et un classement par équipe facultatif ; le nom et le logo de l'organisation sur les certificats des enfants ; connexion facultative du personnel via le fournisseur d'identité du Responsable (OpenID Connect).
Finalité	Dispenser une éducation au développement durable fondée sur les Objectifs de développement durable des Nations unies, avec le suivi de la progression, les rapports et l'évaluation prévus par la Licence. Pour les études d'impact : l'évaluation par le Responsable du traitement de son enseignement (résultats de classe pour ses enseignants) et des statistiques agrégées et anonymisées au titre de la clause 2.3. Aucune autre finalité.
Catégories de personnes concernées	Élèves (le jeu est conçu pour les 9–17 ans en deux tranches d'âge, 9–12 et 13–17 ; les fiches pédagogiques imprimables couvrent les tranches 6–10, 11–13 et 14–17 ans, et le Responsable du traitement peut utiliser le Service avec des élèves plus jeunes selon sa propre appréciation) ; enseignants ; administrateurs d'établissement ; parents et représentants légaux, uniquement lorsque la procédure de consentement est utilisée ; pour les licences entreprises et hôtels, les enfants des salariés ou des clients, et les coordinateurs de l'organisation.

Élément	Description
Données à caractère personnel — élèves (site web, dans une classe)	Prénom ou pseudonyme saisi par l'élève ou par l'enseignant (2 à 24 caractères ; issu des importations de listes, le prénom suivi de l'initiale, étendue au plus aux 3 premières lettres du nom de famille uniquement pour distinguer deux élèves portant le même prénom — jamais le nom complet) ; tranche d'âge choisie dans le jeu (9–12 ou 13–17) ; avatar parmi un ensemble fixe ; langue ; progression (points, objectifs et missions accomplis, étoiles du quiz, nombre de questions répondues et réussies par thème) ; devoirs accomplis ; date d'inscription et de dernière activité ; un jeton de classe aléatoire enregistré sur l'appareil de l'élève pour pouvoir sauvegarder la progression. Dans un quiz de classe en direct : le pseudonyme saisi, les réponses, les temps de réponse et le score. Ne sont pas collectés : adresse e-mail, nom de famille, photographie, date de naissance, adresse postale, localisation, identifiants d'appareil ou publicitaires.
Données à caractère personnel — élèves (lancements LTI)	Un hachage à clé de l'identifiant utilisateur de la plateforme (pour associer un élève à une place) ; l'identifiant utilisateur de la plateforme dans l'enregistrement de lancement pendant 90 jours, uniquement lorsque la plateforme a accordé le service de notes (nécessaire à la remontée des scores) ; prénom et initiale du nom comme pseudonyme ; identifiant et intitulé du cours ; rôles ; paramètres régionaux ; dernier score transmis. Aucune adresse e-mail ni aucun nom complet n'est enregistré ; le Responsable du traitement configure sa plateforme pour ne partager que le nom.
Données à caractère personnel — élèves (application mobile, tableau de bord de classe)	Activité (jeu quotidien joué, date, langue, points, achèvement, durée ; objectifs atteints, badges) et un hachage à sens unique d'un identifiant d'installation aléatoire généré par l'application. Les élèves apparaissent à l'enseignant sous un pseudonyme généré. Le tableau de bord n'affiche rien pour une classe de moins de cinq élèves actifs.
Données à caractère personnel — élèves (étude d'impact, lorsque le Responsable du traitement inscrit une classe)	Réponses au questionnaire de l'étude (choix, notes et courtes réponses facultatives en texte libre), version du questionnaire, langue, tranche d'âge, heures de début et d'envoi et indicateurs de qualité. Les adresses e-mail et numéros de téléphone sont supprimés du texte libre à réception. Les réponses susceptibles de contenir une révélation relevant de la protection de l'enfance sont signalées au référent désigné par le Responsable du traitement. Les réponses sont reliées entre les vagues de l'étude par un hachage à sens unique et à clé de la place de l'élève dans la classe ; aucun nom, aucune adresse e-mail ni aucune date de naissance n'est collecté. Pour chaque place, l'opposition ou le consentement écrit enregistré par le Responsable du traitement. Si aucun référent en matière de protection de l'enfance n'est désigné, les destinataires prévus à la clause 4.4 en tiennent lieu.
Données à caractère personnel — enseignants et administrateurs d'établissement	Nom, adresse e-mail professionnelle, établissement, rôle (enseignant ou administrateur d'établissement), langue ; mot de passe (hachage bcrypt) ou identifiant d'authentification unique ; secret d'authentification à deux facteurs et codes de secours hachés en cas d'activation (obligatoire pour les administrateurs d'établissement) ; statut de vérification de l'e-mail ; heures et nombre de connexions ; sessions ; classes créées ; aperçus d'importation de listes (noms uniquement, conservés dans la session pendant 30 minutes) ; entrées du journal d'audit des actions administratives (avec un hachage à clé de l'adresse IP et le pays de la connexion sous forme de code à 2 lettres fourni par le réseau de diffusion de contenu) ; correspondance d'assistance.

Élément	Description
Données à caractère personnel — enseignants (étude d'impact)	Réponses au questionnaire enseignant et, pour les élèves de 6 à 8 ans, la fiche d'observation de la classe, reliées par un hachage à sens unique et à clé du compte ou du code de l'enseignant ; l'inscription de la classe, son mode de consentement et son affectation à un groupe de l'étude.
Données à caractère personnel — parents et représentants légaux	Uniquement lorsque la procédure de consentement parental du site web est utilisée pour un élève n'ayant pas atteint l'âge du consentement numérique : un hachage à sens unique et à clé de l'adresse e-mail du parent (l'adresse elle-même n'est utilisée qu'une fois pour envoyer le lien de confirmation et n'est pas enregistrée), la décision et ses horodatages.
Données à caractère personnel — enfants et coordinateurs (licences entreprises et hôtels)	Enfants des salariés ou des clients du Responsable du traitement : ils rejoignent un groupe avec le code d'accès du Responsable du traitement et un nom de héros (pseudonyme) sur leur propre appareil ou celui de leur famille, sans compte et sans adresse e-mail. Le Service conserve les mêmes données que pour les élèves d'une classe : nom de héros, tranche d'âge, avatar, langue, progression et résultats des quiz. Coordinateurs : nom, adresse e-mail professionnelle, hachage du mot de passe ou identifiant de connexion, paramètres d'authentification à deux facteurs et groupes qu'ils ouvrent. Le coordinateur voit les objectifs atteints et les résultats des quiz par groupe et peut les exporter au format CSV. Pour le rapport de l'organisation, le Service enregistre aussi, pour chaque profil de héros de ces groupes, les jours d'activité et le jour où chaque objectif ou mission a été terminé pour la première fois (à la journée près ; les classes des écoles ne sont pas suivies ainsi). Les rapports ne contiennent que des agrégats : aucun nom, pseudonyme, identifiant ni ligne par enfant ; tout chiffre reposant sur 1 à 4 familles est masqué (k = 5), et un second chiffre est masqué lorsqu'un seul permettrait de le déduire. Les noms des équipes sont choisis par l'administrateur du Responsable et ne doivent pas désigner des personnes. Lorsque le Responsable active la connexion d'entreprise, les noms et adresses e-mail du personnel proviennent du fournisseur d'identité du Responsable (portées openid, email et profile) ; ce fournisseur d'identité est un système et un sous-traitant du Responsable lui-même, et non un Sous-traitant ultérieur, et son identifiant de sujet n'est conservé que sous forme de hachage à clé. Coaffichage de marque : le nom d'affichage et le logo de l'organisation, fournis par le Responsable. La page publique du badge qu'un parent ou un tuteur peut partager sur LinkedIn ne contient aucune donnée personnelle (un nombre d'objectifs, le nom de l'organisation si le Responsable l'a activé, et une langue, le tout tiré de son lien) ; c'est l'adulte qui lance le partage, et le Sous-traitant n'envoie rien à LinkedIn.
Catégories particulières (article 9 du RGPD)	Aucune n'est demandée ni nécessaire. Voir la clause 4.2.
Fréquence	Continue, pendant la durée de la Licence.

B. Traitements dont Eco Heroes est responsable de manière indépendante (hors du présent Accord)

Mentionnés pour que le Responsable du traitement voie où s'arrête le présent Accord. Ils relèvent de la Politique de confidentialité (v4.3) et de la Notice de confidentialité pour les enfants (v2.2) du Sous-traitant, et non du présent Accord :

- **Les comptes enseignants en tant que tels :** connexion, sécurité, authentification à deux facteurs et ressources gratuites pour enseignants. Le Sous-traitant est responsable du compte lui-même et le

supprime comme le prévoit la clause 10.4 ; l'activité du compte pour le Responsable du traitement constitue des Données du Responsable.

- **Comptes enseignants gratuits :** enseignants non rattachés à une licence qui utilisent les ressources gratuites pour enseignants avec une adresse e-mail vérifiée.
- **Abonnements famille** souscrits sur le site web par un parent ou un représentant légal : l'adresse e-mail (enregistrée partiellement masquée), les références de paiement et d'abonnement Stripe et un code d'accès personnel (enregistré sous forme de hachage à clé). Les données de carte ne parviennent jamais au Sous-traitant. Un code famille utilisé à l'école ne porte aucune donnée de l'établissement.
- **Comptes de l'application** (connexion des parents avec Google ou Apple ; abonnements via Google Play ou Apple ; statut de l'abonnement via RevenueCat).
- **Visiteurs du site web** sur les pages publiques destinées aux adultes (Google Analytics 4 après consentement ; le formulaire de contact via Formspree ; les demandes de devis et les candidatures d'ambassadeurs via le propre serveur du Sous-traitant ; les e-mails Dinner Questions via Brevo).
- **Classement public du quiz** (facultatif : un pseudonyme choisi dans une liste générée, le score et un hachage à clé de l'adresse IP ; conservé 30 jours).
- **Enquêtes du programme** que le Sous-traitant mène hors d'une classe, avec le consentement d'un parent lorsque la loi l'exige.
- **Services distincts :** Eco Heroes Academy (learn.eco-heroes.org) et l'évaluation VSME (assessment.eco-heroes.org) disposent de leurs propres conditions et informations sur la confidentialité.

C. Calendrier de conservation (tel qu'appliqué dans le Service)

Annexe I.C — calendrier de conservation

Données	Conservation	Mécanisme
Données des élèves et des enfants des groupes d'entreprises et d'hôtels (pseudonyme, tranche d'âge, avatar, progression, devoirs, activité de classe dans l'application, association des places LTI)	Pendant la Licence : jusqu'à ce qu'un enseignant ou un administrateur supprime l'élève ou la classe. Après la fin de la Licence : suppression 90 jours après la date de fin, sauf renouvellement de la Licence. Sur demande écrite du Responsable du traitement : suppression dans un délai de 30 jours ; les administrateurs de l'établissement sont prévenus par courriel 30 et 7 jours avant la suppression	Action de l'enseignant ou de l'administrateur dans le Service ; suppression automatique en fin de licence ; le Sous-traitant sur demande écrite
Dates d'activité des profils de héros dans les groupes d'entreprise et d'hôtel (rapport de l'organisation)	Conservées avec le profil de héros et supprimées avec lui, selon la règle ci-dessus	Suppression avec le profil
Réglages de l'organisation : noms des équipes et équipe de chaque groupe, activation du classement par équipe, nom et logo du coaffichage, configuration de la connexion d'entreprise	Pendant la durée de la Licence ; supprimés à la demande du Responsable	Sous-traitant, sur demande

Données	Conservation	Mécanisme
Connexion d'entreprise : enregistrements du processus de connexion ; liens d'identité fixés (hachage à clé du sujet du fournisseur d'identité)	Enregistrements du processus : supprimés à l'usage ou après 10 minutes. Liens d'identité : jusqu'à la suppression du compte ou la suppression ou réinitialisation de la configuration de connexion du Responsable	Purge automatique ; action d'un administrateur
Quiz de classe en direct (pseudonymes, réponses, temps, scores)	30 jours après la création de la session du quiz	Purge quotidienne automatique
Aperçus d'importation de listes (OneRoster)	30 minutes, uniquement dans la session serveur de l'enseignant	Expiration de la session
Jeton d'accès Google Classroom (importation de listes)	Uniquement pendant l'importation, dans la session de l'enseignant ; jamais écrit dans la base de données	Expiration de la session
Enregistrements de lancement LTI	Lancements enseignants, et lancements élèves sans service de notes : 2 heures. Lancements élèves avec service de notes : 90 jours	Purge automatique lors de l'activité LTI
État de connexion LTI, jetons de transfert, jetons de liens profonds, nonces, jetons d'importation de listes	10 minutes / 10 minutes / 60 minutes / 15 minutes / 2 heures	Purge automatique ; usage unique
Comptes enseignants, coordinateurs et administrateurs d'établissement	12 mois après la fin de la dernière licence liée au compte ; comptes gratuits après 12 mois sans connexion ; e-mail d'avertissement 30 jours avant la suppression. Inscriptions non vérifiées : supprimées 7 jours après l'expiration du dernier lien de confirmation	Purge automatique des comptes
Sessions et « se souvenir de moi »	Session serveur pendant sa durée configurée, renouvelée à la connexion et toutes les 30 minutes ; toutes les sessions prennent fin lors d'un changement de mot de passe ou lorsqu'un administrateur retire l'accès. Cookie « se souvenir de moi » : 180 jours (signé HMAC)	Code
Enregistrements de limitation de débit (tentatives de connexion et autres limites)	30 jours	Purge quotidienne automatique
Journal d'audit de sécurité (actions administratives, activations de codes et connexions ; hachage à clé de l'IP, pays de la connexion en code à 2 lettres)	12 mois	Purge quotidienne automatique
Hachages d'IP anti-abus sur les réponses aux enquêtes et les demandes de consentement	30 jours (la réponse elle-même suit sa propre durée)	Purge quotidienne automatique

Données	Conservation	Mécanisme
Demandes de consentement parental	Sans réponse ou expirées : 30 jours. Refus : 12 mois. Consentement donné : tant qu'il est invoqué ; effacé avec les données en cas de retrait du consentement	Purge quotidienne automatique ; fonction d'effacement
Réponses aux études d'impact (élèves, enseignants, fiches d'observation) et marques d'opposition ou de consentement	24 mois après la clôture de la dernière vague de l'étude ; plus tôt sur instruction écrite du Responsable du traitement. Les marques d'opposition et de consentement sont supprimées avec l'inscription de la classe	Purge quotidienne automatique ; le Sous-traitant sur demande écrite
Signalements de protection de l'enfance (réponses aux études d'impact pouvant contenir une révélation, avec la place et le pseudonyme auxquels elles se rattachent)	Le texte de la réponse est effacé 30 jours après que le signalement a été marqué comme traité ; l'enregistrement du signalement est supprimé 12 mois après son traitement	Purge quotidienne automatique
Réponses aux enquêtes du programme	24 mois, ou jusqu'au retrait du consentement	Purge quotidienne automatique ; fonction d'effacement
Entrées du classement public du quiz (hors du présent Accord, mentionnées pour être complet)	30 jours	Purge quotidienne automatique
Traces de l'acceptation du présent Accord par le Responsable du traitement (qui l'a accepté, quand, quelle version, hachage à clé de l'adresse IP ; conservées par le Sous-traitant en tant que responsable du traitement, clause 13.3)	Pendant toute la durée de la Licence et 6 ans après sa fin	Registres du Sous-traitant
Traces d'acceptation lors du paiement, de résiliation et de rétractation des offres famille (hors du présent Accord, mentionnées pour être complet)	6 ans, avec les documents comptables (code de commerce espagnol, article 30)	Documents comptables
Compteur de taux de participation dérivé d'une personne	2 jours	Purge quotidienne automatique
Télémétrie (rapports de violations de CSP et d'erreurs JavaScript)	Aucun identifiant enregistré (agent utilisateur tronqué) ; compteurs de limitation réinitialisés chaque minute ; journal plafonné à 5 Mo	Code
Correspondance d'assistance (e-mail)	Jusqu'au traitement de la demande, et au plus 12 mois après le dernier message	Procédure de la messagerie du Sous-traitant
Sauvegardes chiffrées	Sauvegardes chiffrées conservées par rotation ; les données supprimées disparaissent de toutes les sauvegardes dans un délai de 14 jours	Automatique

Données	Conservation	Mécanisme
Réplique de secours de la base de données	En continu ; suit chaque suppression	Réplication
Journaux techniques du serveur web (adresse IP, adresse demandée)	Jusqu'à 90 jours	Configuration du serveur
Factures et documents de paiement	6 ans (code de commerce espagnol, article 30) ; ils identifient les personnes de contact du Responsable du traitement, jamais les élèves	Documents comptables

Annexe II — Mesures techniques et organisationnelles (article 32 du RGPD)

Les mesures en place à la date du présent Accord. Elles sont revues à chaque version, et la synthèse en vigueur est publiée à l'adresse https://eco-heroes.org/trust/#security. Le Sous-traitant peut mettre à jour les mesures, à condition que le niveau global de sécurité ne diminue pas.

1. Chiffrement en transit

- TLS 1.2 ou supérieur pour toutes les connexions ; HTTP Strict Transport Security avec un max-age de deux ans, includeSubDomains et preload ; renouvellement automatique des certificats ; certificats d'origine entre le réseau de diffusion de contenu et les serveurs.
- Les serveurs d'application ne se connectent à la base de données qu'en TLS 1.2/1.3, avec vérification du certificat par rapport à une autorité de certification épinglée ; la base de données refuse les connexions non chiffrées (require_secure_transport). Les comptes de la base de données sont limités aux hôtes d'application et de secours.
- Les sauvegardes sont chiffrées (AES-256-CBC, PBKDF2 avec 200 000 itérations) avant de quitter le serveur et ne circulent que par des connexions chiffrées. Aucune archive non chiffrée n'est écrite.

2. Protection côté navigateur

- Content-Security-Policy : les scripts en ligne ne s'exécutent que s'ils sont approuvés par un hachage SHA-256 par script, ou par un nonce par requête sur quelques pages dynamiques (pas d'unsafe-inline pour les scripts — les styles en ligne restent autorisés ; object-src 'none', base-uri 'self', frame-ancestors 'none' sauf pour les pages LTI, que seules les plateformes d'apprentissage enregistrées peuvent intégrer). Les rapports de violation sont collectés, avec limitation de débit. Les pages destinées aux enfants ne chargent aucun script tiers. Sur les pages pour adultes, les seuls scripts tiers sont Google Analytics, après consentement, et la vérification Cloudflare Turnstile sur les formulaires de connexion et d'inscription.
- Les polices web sont hébergées sur le propre serveur du Sous-traitant. Aucune requête n'est envoyée à Google Fonts ni à aucun autre fournisseur de polices.
- En-têtes de sécurité : X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy et Cross-Origin-Resource-Policy same-origin. Les en-têtes de version du serveur et de PHP sont supprimés. HTTP TRACE et TRACK sont refusés.
- Cookies : le cookie de session est Secure, HttpOnly et SameSite=Strict, en mode de session strict ; l'identifiant de session change à la connexion, à l'activation d'un code et toutes les 30 minutes. Le cookie « se souvenir de moi » est signé HMAC avec une clé côté serveur. Le cookie d'état LTI est limité à /lti/ et partitionné.
- Le service worker des jeux ne met jamais en cache les réponses marquées no-store ou private, ni aucun chemin réservé aux membres, de sorte qu'aucun contenu réservé ne reste dans le cache d'un appareil partagé après la déconnexion.
- Les réponses contenant des données à caractère personnel ou du contenu réservé aux membres sont envoyées avec Cache-Control: private, no-store, et le réseau de diffusion de contenu ne les met jamais en cache.

3. Contrôle d'accès et authentification

- Comptes enseignants nominatifs : un code d'établissement ne sert qu'une fois, pour l'inscription. Il crée un compte nominatif avec une adresse e-mail vérifiée, ou rattache l'établissement au compte que

l'enseignant possède déjà. Ensuite, l'enseignant se connecte avec sa propre adresse e-mail et son mot de passe, ou par authentification unique. Un appareil sur lequel seul un code d'établissement a été saisi peut jouer, mais n'a pas accès aux outils pour enseignants. Un code d'administration ne crée que le premier compte administrateur de l'établissement et est épuisé dès que ce compte est confirmé ; les enseignants rejoignent ensuite l'établissement avec un code du personnel qu'un administrateur crée dans le Service, affiché une seule fois, enregistré uniquement sous forme de hachage à clé et remplaçable à tout moment.

- Les mots de passe des enseignants sont hachés avec bcryptet comparés en temps constant. L'adresse e-mail doit être vérifiée avant la première connexion. Le changement de mot de passe met fin à toutes les sessions. Un administrateur d'établissement peut retirer immédiatement l'accès d'un enseignant.
- L'authentification à deux facteurs (TOTP, avec codes de secours hachés) est obligatoire pour les administrateurs d'établissement et les super-administrateurs du Sous-traitant, et tout enseignant ou coordinateur d'une licence entreprise ou hôtel peut l'activer. Le QR code d'enrôlement est généré sur le serveur, de sorte que le secret ne le quitte jamais. Le second facteur est vérifié avant la création de toute session, et les administrateurs d'établissement doivent l'utiliser partout où des données d'élèves sont visibles. Le référent en matière de protection de l'enfance doit également l'utiliser pour lire les signalements. Après 10 codes erronés en 24 heures, le second facteur du compte est bloqué pendant 15 minutes et le titulaire du compte en est informé par e-mail.
- Les codes d'accès ne sont enregistrés que sous forme de hachages à clé dans un fichier situé hors de la racine web ; la clé est conservée hors de la racine web. Les codes d'inscription et de licence sont enregistrés de la même manière ; un code n'est affiché qu'une fois, lors de sa création.
- Limitation de débit sur la connexion (par adresse IP et par couple e-mail/IP, avec un plafond global), l'inscription, l'utilisation des codes, l'entrée dans une classe, l'entrée dans un quiz en direct, la synchronisation de la progression, le formulaire de devis, les connexions LTI, les points de télémétrie et les consultations de retour Stripe. Jetons CSRF sur tout formulaire modifiant des données. Protection contre les redirections ouvertes sur chaque paramètre next=.
- Droits d'accès vérifiés côté serveur : les ressources réservées aux membres (vidéos des missions, banques de questions du quiz, livres, contenu LTI) ne sont délivrées qu'après vérification côté serveur d'une session de code valide, d'un code mémorisé signé ou d'un compte connecté. Rien de ce que le navigateur écrit lui-même ne donne accès.
- Isolation par rôle et par établissement : chaque enseignant ne voit que ses propres classes ; les administrateurs d'établissement voient toutes les classes de leur propre établissement et rien des autres établissements ; les enseignants passant par LTI ne voient que les classes du cours depuis lequel ils se sont lancés ; l'accès super-administrateur est limité au personnel nommément désigné du Sous-traitant.
- Toutes les requêtes à la base de données utilisent des requêtes préparées ; pas d'exec, d'eval ni d'unserialize ; les chemins de fichiers ne sont construits qu'à partir d'éléments d'une liste autorisée ; les envois (fichiers CSV/ZIP de listes de classe, images d'enquêtes) sont limités en taille, leur type est vérifié et ils sont stockés hors de la racine web ; l'affichage des erreurs PHP est désactivé.
- Authentification unique facultative pour le personnel des entreprises et des hôtels via OpenID Connect (Authorization Code avec PKCE ; jetons d'identité signés, vérifiés pour l'émetteur, l'audience, l'expiration et le nonce). Les secrets client sont chiffrés au repos. Les comptes ne sont rapprochés qu'au sein des domaines de messagerie autorisés du Responsable et ne sont jamais rattachés au compte d'une autre organisation.

4. Minimisation des données et données des enfants

- Aucune adresse e-mail, aucun nom de famille, aucune photographie, date de naissance, adresse postale, localisation ni aucun identifiant d'appareil ou publicitaire des élèves n'est collecté. Les importations de listes conservent le prénom et au plus les 3 premières lettres du nom de famille. Les élèves passant par LTI sont enregistrés sous un hachage à clé de l'identifiant utilisateur de la plateforme, avec prénom et initiale ; le Responsable du traitement configure sa plateforme pour ne partager que le nom.
- Les adresses IP ne sont enregistrées que sous forme de hachages à clé (préfixe). Le détenteur de la clé pourrait les relier à nouveau ; elles sont donc pseudonymisées, et non anonymes. Lorsqu'elles accompagnent un contenu, elles sont supprimées au bout de 30 jours.
- Les pages destinées aux enfants (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books et leurs versions linguistiques) ne chargent aucune mesure d'audience et n'affichent aucun bandeau de consentement. Sur les autres pages, la mesure d'audience ne se charge qu'après consentement explicite.
- Les vidéos des missions réservées aux membres sont hébergées par le Sous-traitant et servies après vérification des droits d'accès. Lorsqu'un lecteur YouTube subsiste (jeu libre), il utilise youtube-nocookie.com et ne se charge que lorsque l'utilisateur appuie sur lecture.
- La publication dans le classement public du quiz est facultative après chaque partie, sous un pseudonyme généré (un adjectif et un animal ; pas de texte libre ni de nom d'établissement). Le classement public affiche le pseudonyme et le score des 10 meilleurs des 30 derniers jours, et les entrées sont supprimées au bout de 30 jours. Chaque ligne publique comporte un lien de signalement ; une ligne signalée trois fois est masquée jusqu'à son examen. Les classements de classe ne sont visibles que par l'enseignant de la classe et les administrateurs de l'établissement, qui peuvent retirer des lignes.
- Les réponses libres sont filtrées automatiquement à l'envoi : les adresses e-mail et les numéros de téléphone sont supprimés, et les réponses qui correspondent à une courte liste de mots pouvant indiquer qu'un enfant est en danger sont retirées des données de l'étude et transmises uniquement à la personne que l'établissement a désignée pour la protection de l'enfance. Les noms ne sont pas supprimés automatiquement ; les chercheurs qui lisent les réponses signalent les noms possibles et ne les mentionnent jamais dans un rapport. Une révélation possible est transmise à la personne désignée par l'établissement dans un délai d'un jour d'école. Si aucun référent en matière de protection de l'enfance n'est désigné, les destinataires prévus à la clause 4.4 en tiennent lieu.
- Les adresses e-mail des parents dans la procédure de consentement ne sont jamais enregistrées en clair ; seul un hachage à clé est conservé.
- Les rapports de l'organisation sont des agrégats : un chiffre reposant sur moins de 5 familles est masqué dans le calcul lui-même, si bien que ni l'écran ni le CSV ne peuvent l'afficher. Seuls les administrateurs de l'organisation, avec la double authentification, peuvent les ouvrir ; chaque consultation et chaque export sont limités en fréquence et journalisés.

5. Disponibilité, sauvegarde et reprise

- Les opérations suivantes s'exécutent automatiquement. Une surveillance indépendante (UptimeRobot, 11 sondes, toutes les 5 minutes) alerte le Sous-traitant en cas d'échec.
- Une sauvegarde chiffrée chaque nuit de la base de données et de l'application ; une copie est conservée dans un centre de données distinct situé dans un autre pays de l'UE. Une restauration est testée automatiquement chaque mois.
- Une sauvegarde avant chaque version, avec une procédure de retour arrière testée ; la version de production précédente est conservée.
- Un serveur de secours détient une copie de l'application et une réplique en direct de la base de données. Si le serveur web principal tombe en panne, un équilibrage de charge avec contrôles de santé bascule le

trafic automatiquement ; si le serveur de base de données tombe en panne, la réplique est promue selon une procédure scriptée et répétée. Les deux ont été testés en octobre 2026.

- Un contrôle horaire de l'infrastructure (état et retard de la réplique, expiration des certificats, espace disque, mises à jour de sécurité en attente, plages d'adresses du réseau de diffusion de contenu). Les mises à jour de sécurité du système d'exploitation s'installent automatiquement. Protection contre les attaques DDoS et les robots en périphérie du réseau.
- L'environnement de préproduction est séparé de la production (utilisateur Unix distinct, pool PHP avec open_basedir, instance de base de données distincte, secrets retirés).

6. Journalisation et surveillance

- Les événements de sécurité (échecs de connexion, utilisations de codes, actions administratives, rapports de violation de CSP, suppressions et purges de conservation) sont journalisés avec des hachages à clé des adresses IP. Le journal d'audit de sécurité est conservé 12 mois et les enregistrements de limitation de débit 30 jours (annexe I, section C).
- L'état du service en direct et chaque interruption sont publiés sur la page publique d'état.

7. Mesures organisationnelles

- L'accès aux systèmes de production est limité à des personnes nommément désignées. Chaque compte administratif (hébergement, serveurs de base de données et de sauvegarde, réseau de diffusion de contenu et DNS, dépôt de code source, surveillance, messagerie) utilise l'authentification à deux facteurs. L'accès aux serveurs se fait par clés SSH. Des pare-feu limitent l'accès à la base de données et au serveur de secours aux hôtes propres du Sous-traitant et aux plages d'adresses du réseau de diffusion de contenu.
- Les modifications sont testées automatiquement (intégration continue ; une version est refusée si le code n'a pas réussi les tests), passent d'abord par la préproduction et sont vérifiées en production après chaque version (47 vérifications en direct). Une revue statique de sécurité de l'application est réalisée et documentée (dernière : 16 octobre 2026).
- Test d'intrusion, octobre 2026 : un test structuré en boîte blanche et en boîte grise de la plateforme (authentification, sessions, contrôle d'accès entre établissements, paiements, exposition de fichiers et de données, limitation des tentatives et cache en périphérie), réalisé par la propre équipe de test du Sous-traitant. Toutes les vulnérabilités critiques, élevées et moyennes relevées ont été corrigées et testées à nouveau avant la mise en production. Un test d'intrusion externe, confié à un cabinet indépendant, est prévu.
- Un canal de signalement des vulnérabilités est publié à l'adresse /.well-known/security.txt. Les signalements font l'objet d'un accusé de réception dans un délai de 5 jours ouvrés, et les problèmes critiques sont corrigés avant tout autre travail.
- Une procédure écrite de gestion des incidents décrit comment le Sous-traitant détecte, contient et consigne une violation de données à caractère personnel et comment il respecte le délai de notification de 48 heures de la clause 9.
- Le Sous-traitant tient un registre des traitements qu'il effectue pour le compte de responsables du traitement (article 30, paragraphe 2, du RGPD) et une évaluation du transfert pour chaque Sous-traitant ultérieur situé hors de l'EEE.
- Les durées de conservation sont définies dans le code qui les applique, de sorte que la durée publiée et la durée appliquée ne peuvent pas diverger.

- Les secrets (clé restreinte Stripe, identifiants d'authentification unique, clés de hachage) sont conservés hors de la racine web et ne sont jamais versés dans le dépôt de code source.

Annexe III — Sous-traitants ultérieurs et services tiers

Le Centre de confiance (https://eco-heroes.org/trust/#subprocessors) présente les deux mêmes listes.

Partie A — Sous-traitants ultérieurs qui traitent des Données du Responsable

Annexe III.A — sous-traitants ultérieurs autorisés

Sous-traitant ultérieur	Ce qu'il fait	Où	Garantie pour le transfert
Internet Girona, sur l'infrastructure d'OVHcloud	Hébergement web	France (UE)	Dans l'UE ; conditions standard de traitement des données du fournisseur
Hetzner Online GmbH, Gunzenhausen, Allemagne	Hébergement de la base de données, serveur de secours et sauvegardes chiffrées	Allemagne et Finlande (UE)	Dans l'UE ; conditions standard de traitement des données de Hetzner
Cloudflare, Inc., San Francisco, États-Unis	Diffusion de contenu, TLS, protection contre les attaques et les robots, vérification Turnstile sur les formulaires de connexion et d'inscription, et basculement automatique en cas de panne	Réseau périphérique mondial ; serveurs d'origine dans l'UE	Conditions standard de traitement des données de Cloudflare avec les clauses contractuelles types (2021/914) ; cadre de protection des données UE–États-Unis lorsque Cloudflare figure sur la liste
Proton AG, Genève, Suisse	Hébergement de la messagerie info@ et security@eco-heroes.org : correspondance d'assistance et relative à la protection des données avec le personnel du Responsable du traitement	Suisse	Décision d'adéquation de la Commission européenne pour la Suisse ; conditions standard de traitement des données de Proton
Google (Google Ireland Ltd / Google LLC) — connexion et importation Classroom uniquement	Uniquement si le Responsable du traitement les active : connexion des enseignants (nom, adresse e-mail, identifiant ; aucune donnée d'élève) ; importation de listes Google Classroom (prénom et nom lus une fois et enregistrés sous la forme prénom et initiale ; le jeton d'accès reste dans la session de l'enseignant)	UE / États-Unis	Conditions Google propres au Responsable du traitement ; conditions standard de traitement des données de Google avec les clauses contractuelles types ; cadre de protection des données UE–États-Unis lorsqu'il figure sur la liste

Sous-traitant ultérieur	Ce qu'il fait	Où	Garantie pour le transfert
Microsoft (Microsoft Ireland Operations Ltd) — connexion uniquement	Uniquement si le Responsable du traitement l'active : connexion des enseignants (identité uniquement ; aucune donnée d'élève)	UE / États-Unis	Conditions Microsoft propres au Responsable du traitement ; DPA Produits et Services de Microsoft avec les clauses contractuelles types ; cadre de protection des données UE–États-Unis lorsqu'il figure sur la liste
Google (YouTube, youtube-nocookie.com)	Lecture de vidéos éducatives sélectionnées lorsqu'un lecteur YouTube est encore utilisé : mode de confidentialité renforcée, chargé uniquement lorsque l'utilisateur appuie sur lecture	UE / États-Unis	Conditions de Google ; cadre de protection des données UE–États-Unis lorsqu'il figure sur la liste
Moodle Pty Ltd (MoodleCloud), Australie-Occidentale	Uniquement si le Responsable du traitement utilise le site de cours Eco Heroes eco-heroes.moodlecloud.com au lieu de sa propre plateforme d'apprentissage : comptes de cours sur ce site et progression que les jeux y transmettent	Hébergement MoodleCloud sur Amazon Web Services	Accord de traitement des données de MoodleCloud avec les clauses contractuelles types (2021/914) pour tout transfert hors de l'EEE

Partie B — Services tiers qui ne traitent pas de Données du Responsable

Mentionnés par transparence. Lorsque des données à caractère personnel sont en jeu, la Politique de confidentialité du Sous-traitant s'applique. Le propre serveur de messagerie du Sous-traitant envoie les e-mails de compte, de vérification et de service ; il ne s'agit pas d'un tiers.

Annexe III.B — services tiers hors du présent Accord

Service	Ce qu'il fait	Où	Pourquoi il est hors du présent Accord
Stripe	Paiements par carte des abonnements famille sur le site web ; le Sous-traitant consulte le statut du paiement et de l'abonnement	UE / États-Unis ; conditions de traitement des données de Stripe avec les clauses contractuelles types ; cadre de protection des données UE–États-Unis	Les abonnés famille sont les propres clients du Sous-traitant ; aucune donnée d'établissement n'est envoyée à Stripe
Google Analytics 4	Statistiques de visite sur les pages publiques pour adultes, uniquement après consentement ; jamais sur les pages destinées aux enfants ni dans l'espace enseignants	UE / États-Unis ; conditions de traitement des données de Google avec les clauses contractuelles types ; cadre de protection des données UE–États-Unis	Aucune Donnée du Responsable n'est envoyée ; le Sous-traitant est responsable de ses propres statistiques web

Service	Ce qu'il fait	Où	Pourquoi il est hors du présent Accord
Formspree	Transmet les messages envoyés avec le formulaire de contact général	États-Unis ; conditions standard de traitement des données du fournisseur (clauses contractuelles types ; cadre de protection des données UE–États-Unis lorsqu'il figure sur la liste)	Les messages sont la correspondance propre du Sous-traitant ; non utilisé par le Service
Brevo	E-mails Dinner Questions pour les familles (sur inscription ; adresse e-mail uniquement)	UE	Lettre d'information pour les familles ; non utilisée par le Service
RevenueCat	Statut de l'abonnement dans l'application (identifiant de compte et historique d'achats uniquement)	États-Unis ; clauses contractuelles types	Comptes famille de l'application ; aucune donnée d'établissement
Google Play / Apple App Store	Paiements d'abonnement dans l'application, encaissés par la boutique	UE / États-Unis	Les boutiques vendent l'abonnement en tant que responsables du traitement indépendants
Google / Apple (connexion dans l'app)	Connexion facultative des parents dans l'application (adresse e-mail et identifiant de connexion)	UE / États-Unis ; cadre de protection des données UE–États-Unis, clauses contractuelles types	Comptes famille de l'application ; aucune donnée d'établissement
UptimeRobot	Vérifie que les pages publiques et le point d'état répondent	UE / États-Unis	Ne traite aucune donnée à caractère personnel

Annexe IV — Données des enfants

La présente annexe complète les annexes I et II pour les élèves de moins de 18 ans.

1. **Âge du consentement numérique.** Lorsque la loi applicable au Responsable du traitement exige un consentement pour les services de la société de l'information proposés directement à un enfant (article 8 du RGPD), le Responsable du traitement l'obtient et le consigne. Cet âge est de 14 ans en Espagne (article 7 de la LOPDGDD), de 13 à 16 ans dans les autres États membres de l'UE et de 13 ans au Royaume-Uni ; pour les établissements des États-Unis, voir l'annexe V. Lorsque le Responsable du traitement se fonde sur une autre base juridique pour l'usage scolaire, par exemple une mission d'intérêt public, aucun consentement n'est nécessaire et le Responsable du traitement informe les élèves et les parents. Le Service ne vérifie pas l'âge. Ses deux tranches d'âge (9–12 et 13–17) ne font que choisir le contenu et la version des vidéos.
2. **Procédure de consentement parental sur le site web.** Lorsqu'une fonction du site web nécessite le consentement d'un parent pour un enfant n'ayant pas atteint l'âge du consentement numérique, le Service n'enregistre rien tant que le parent n'a pas confirmé au moyen d'un lien à usage unique envoyé par e-mail. Seuls sont enregistrés un hachage à clé de l'adresse e-mail du parent, la décision et les horodatages. Les demandes sans réponse sont supprimées au bout de 30 jours et les refus au bout de 12 mois. Le retrait du consentement efface les données recueillies sur son fondement.
3. **Offre famille.** Un parent ou représentant légal souscrit l'abonnement famille et est client du Sous-traitant. Sur le site web, le paiement demande à l'acheteur de confirmer qu'il est majeur ; dans l'application, les étapes de connexion et d'achat se trouvent derrière un contrôle adulte (une question de calcul à saisir). Ni l'un ni l'autre ne constitue une vérification d'identité ou d'âge. Les enfants n'ouvrent pas de compte sur le site web. Un enfant peut utiliser un code famille sous la responsabilité de son parent ; aucune donnée d'établissement n'y est rattachée.
4. **Pas de profilage ni de publicité.** Le Sous-traitant n'affiche aucune publicité et n'utilise aucun identifiant ni SDK publicitaire. Il n'établit pas de profils d'élèves au-delà du suivi de la progression que voient les enseignants du Responsable du traitement, ne prend aucune décision automatisée produisant des effets juridiques ou des effets significatifs similaires, et ne vend ni ne partage jamais de données d'élèves à des fins publicitaires.
5. **Pas de mesure d'audience sur les pages pour enfants.** Les pages destinées aux enfants (le jeu d'aventure, l'espace jeux, le quiz, la bibliothèque, les pages des objectifs, Wordle, les missions et les livres, dans les 13 langues) ne chargent aucune mesure d'audience, aucun traceur ni aucun bandeau de consentement. Elles n'utilisent que le stockage du navigateur strictement nécessaire (langue, progression sur l'appareil, session).
6. **Études d'impact.** Lorsque le Responsable du traitement inscrit des classes à une étude d'impact, les élèves répondent en classe dans le cadre de l'évaluation que le Responsable du traitement fait lui-même de son enseignement. Le Responsable du traitement informe les parents à l'avance et leur offre la possibilité de s'opposer, ou recueille un consentement écrit lorsque sa loi ou ses règles l'exigent ; le Service permet les deux et exclut les places concernées. Les élèves peuvent passer toute question et en sont informés sur le premier écran. Les enseignants ne voient que des résultats de classe, et seulement lorsqu'au moins 10 élèves ont répondu avant et après ; aucun utilisateur de l'établissement ne voit les réponses individuelles d'un élève. Une réponse en texte libre susceptible de contenir une révélation relevant de la protection de l'enfance est transmise au référent désigné par le Responsable du traitement, qui décide de la suite à donner. Le Sous-traitant n'utilise que des résultats agrégés et anonymisés au titre de la clause 2.3, jamais de texte libre. Une révélation possible est transmise au référent désigné dans un

délai d'un jour d'école, et seul ce référent la voit. Si aucun référent en matière de protection de l'enfance n'est désigné, les destinataires prévus à la clause 4.4 en tiennent lieu.

7. **Pas de fonctions de communication.** Le Service ne comporte ni messagerie instantanée, ni messagerie, ni profils publics d'élèves. Le classement public du quiz est facultatif, n'utilise que des pseudonymes choisis dans une liste générée, n'affiche aucun nom d'établissement, conserve les entrées 30 jours et comporte un lien de signalement sur chaque entrée. Les classements de classe ne sont visibles que par l'enseignant de la classe et les administrateurs de l'établissement, et une entrée publique signalée trois fois est masquée jusqu'à son examen.
8. **Risque résiduel communiqué au Responsable du traitement.** Un camarade qui connaît un code de classe et le pseudonyme d'un élève peut ouvrir la progression de cet élève sur un autre appareil. Les enseignants peuvent voir, renommer ou retirer des élèves à tout moment et peuvent renouveler le code de classe. Le Responsable du traitement en tient compte dans sa propre évaluation et dans sa manière de distribuer les codes de classe.
9. **Droits des parents et des élèves.** Les parents et les élèves exercent leurs droits auprès du Responsable du traitement. Les enseignants du Responsable du traitement peuvent consulter, exporter, renommer, réinitialiser et supprimer directement les données d'un élève. Le Sous-traitant transmet au Responsable du traitement toute demande qu'il reçoit (clause 8.2).
10. **Information des enfants.** Le Sous-traitant publie une Notice de confidentialité pour les enfants comprenant une partie rédigée pour les enfants (partie A) et une partie pour les parents et les établissements (partie B) à l'adresse https://eco-heroes.org/legal/children/. Le Responsable du traitement peut la reprendre dans sa propre information aux élèves et aux parents.

Annexe V — Responsables du traitement au Royaume-Uni et aux États-Unis

1. **Royaume-Uni.** Lorsque le Responsable du traitement est établi au Royaume-Uni, les références du présent Accord au RGPD s'entendent comme faites au UK GDPR et au Data Protection Act 2018, et l'autorité de contrôle compétente est l'Information Commissioner's Office (ICO). Les Données du Responsable sont transférées du Royaume-Uni vers l'EEE en vertu des règlements d'adéquation du Royaume-Uni pour l'EEE. Les transferts ultérieurs vers les États-Unis reposent sur l'extension britannique du cadre de protection des données UE–États-Unis lorsque le fournisseur est certifié, ou sur l'avenant britannique relatif aux transferts internationaux de données (UK International Data Transfer Addendum) aux clauses contractuelles types. Le Sous-traitant conçoit le Service en tenant compte de l'Age Appropriate Design Code de l'ICO ; sa synthèse de conformité figure à la section 11 de la Politique de confidentialité.
2. **États-Unis — FERPA.** Lorsque le Responsable du traitement est un établissement ou un district scolaire des États-Unis soumis au Family Educational Rights and Privacy Act, le Sous-traitant agit en tant que « school official » ayant un intérêt éducatif légitime au sens de 34 CFR 99.31(a)(1)(i)(B). Le Sous-traitant est placé sous le contrôle direct du Responsable du traitement pour l'utilisation et la tenue des dossiers scolaires, ne les utilise qu'aux fins de la Licence et ne les communique à personne d'autre, sauf aux Sous-traitants ultérieurs au titre de la clause 6 ou lorsque la loi l'exige.
3. **États-Unis — COPPA.** Pour les élèves de moins de 13 ans, le Responsable du traitement peut consentir au nom des parents à la collecte des données décrites à l'annexe I, comme le permettent les lignes directrices de la Federal Trade Commission, car les données ne sont utilisées qu'aux fins éducatives du Responsable du traitement et à aucune autre fin commerciale. Le Responsable du traitement tient les parents informés et transmet leurs demandes de consultation ou de suppression des données de leur enfant ; le Sous-traitant y donne suite au titre de la clause 8.

4. **États-Unis — suppression et notification.** La clause 10 s'applique à la suppression en fin de Licence. Lorsqu'une loi d'un État sur la protection des données des élèves fixe un délai plus court pour la notification des violations ou la suppression, le Sous-traitant le respecte dès que le Responsable du traitement lui indique quelle loi s'applique.
