本書は便宜のために提供される翻訳です。英語版が法的拘束力を有する正文であり、両者の間に相違がある場合は英語版が優先します。 English (PDF)

データ処理契約

規則（EU）2016/679（GDPR）第28条および個人データの保護およびデジタル権利の保障に関する12月5日付スペイン組織法3/2018（LOPDGDD）第33条に基づき、ライセンス保有者（以下「管理者」）とEco Heroes International SL（以下「処理者」）との間で締結される契約

当事者および役割

管理者：_____（本ライセンスに記載された学校、学校グループ、教育行政機関、企業またはホテルの名称）、登録住所 _____、代表者 _____（氏名、役職）。
データ保護に関する管理者の連絡先（管理担当者の連絡先、または任命されている場合はデータ保護責任者）：_____。

処理者：Eco Heroes International SL、CIF B44915940、登録事務所 17003 Girona（スペイン）、Registro Mercantil de Girona に登記、代表者 創業者 Karim Zouhdi。データ保護に関する連絡先：info@eco-heroes.org、+34 690 814 215。セキュリティに関する報告：security@eco-heroes.org（https://eco-heroes.org/.well-known/security.txt を参照）。

役割。管理者は、管理者データを処理する目的および方法を決定し、その管理者となる。処理者は、GDPR第4条第8号に定める処理者として、管理者に代わってのみ管理者データを処理する。

教師アカウント。各教師は、本人名義の個人アカウントを持つ。処理者は、アカウントそのもの（ログイン、セキュリティ、二段階認証および無料の教師向け教材）を、自らのプライバシーポリシーに基づき管理者として運営する。教師が管理者のために本サービス内で行うことはすべて管理者データとなる。すなわち、管理者の組織におけるアカウントの役割および権限、クラス、児童・生徒、進捗、宿題、ライブクイズ、名簿インポート、学習プラットフォームからの起動および効果測定調査である。

本契約の対象外。附属書I第B節に、処理者自身が管理者となる処理を掲げる。これらは処理者のプライバシーポリシー（https://eco-heroes.org/legal/privacy/）の対象であり、本契約の対象ではない。Eco Heroes Academy（learn.eco-heroes.org）およびVSME評価（assessment.eco-heroes.org）は、独自の規約およびプライバシーに関する情報を有する別個のサービスであり、本契約の対象ではない。

本契約は本ライセンスの一部を構成する。個人データの処理に関して本ライセンスと本契約とが抵触する場合は、本契約が優先する。

定義

- **「本ライセンス」**：管理者が本サービスを利用する根拠となる契約をいう。管理者が承諾した見積書または注文書、および https://eco-heroes.org/legal/licence/ に掲載する学校および組織向けライセンス条件から成る。
- **「本サービス」**：第1.1条に記載するEco Heroesプラットフォームおよびサポートをいう。
- **「管理者データ」**：附属書I第A節に記載するとおり、処理者が本契約に基づき管理者に代わって処理する個人データをいう。
- **「利用者」**：管理者が本サービスの利用を認めた児童・生徒、教師、学校の管理担当者、職員、従業員、宿泊客その他の者をいう。
- **「再委託先」**：処理者が管理者データの処理のために使用する他の処理者をいう。
- **「営業日」**：月曜日から金曜日までをいう。ただし、Girona（スペイン）の祝日を除く。
- GDPR第4条に定義される用語（「個人データ」、「処理」、「個人データ侵害」など）は、本契約においても同じ意味を有する。

1. 対象事項および期間

1.1 処理者は、本ライセンスに基づき管理者に本サービスを提供する。本サービスには、アドベンチャーゲーム、クイズ、単語ゲームおよびクラスでのライブクイズ、絵本およびストーリーライブラリー、ミッション動画、ハンドブックおよび授業シート、本人名義の教師アカウント、クラス管理および宿題、任意の名簿インポート（CSV、OneRoster CSV、Google Classroom）、GoogleまたはMicrosoftによる任意の教師ログイン、LTI 1.1またはLTI 1.3による管理者の学習プラットフォームとの任意の連携、管理者が利用する場合のEco Heroesモバイルアプリのクラスダッシュボード、任意の効果測定調査、企業およびホテル向けライセンスにおけるコーディネーターアカウント、従業員または宿泊客の子どものためのアクセスコード付きグループおよびグループごとの進捗レポート（CSV）、組織の集計レポート、組織名入りの修了証、管理者自身のIDプロバイダーによるスタッフの任意のサインイン、ならびにサポートが含まれる。

1.2 処理者は、本ライセンスの期間中、および第10条に基づきすべての管理者データが削除または返還されるまで、管理者データを処理する。

2. 処理の性質および目的；種類

2.1 処理の性質および目的、データ主体の種類ならびに個人データの種類は、**附属書I**に定める。

2.2 処理者は、管理者に本サービスを提供する目的のためにのみ管理者データを処理する。処理者は、管理者データを、広告のため、本サービスが管理者の教師に表示する学習進捗を超えて児童・生徒のプロファイルを作成するため、データを販売もしくは貸与するため、または本サービス以外の製品を開発するために使用しない。

2.3 **匿名化された統計。**管理者がクラスを効果測定調査に登録する場合、管理者は、回答から集計統計を作成することを処理者に指示し、処理者はこれを自らの報告書および出版物に使用することができる。処理者は、10人以上の児童・生徒のグループの回答のみを集計し、自由記述の回答を一切含めず、いかなる児童・生徒、クラスまたは学校も特定できないことを確認する。このように作成された統計は、もはや個人データではない。管理者は、書面による通知により、いつでもこの指示を撤回することができる。その後に収集された回答は、管理者自身の結果のためにのみ使用される。

3. 指示

3.1 処理者は、第三国または国際機関への移転に関するものを含め、管理者からの文書化された指示に基づいてのみ管理者データを処理する。ただし、処理者が服するEU法または加盟国法により処理が義務付けられる場合はこの限りでない。この場合、処理者は、当該法が重要な公共の利益を理由としてその通知を禁止しない限り、処理に先立って当該法的要件を管理者に通知する。

3.2 管理者の文書化された指示とは、本契約、本ライセンス、ならびに管理者およびその利用者が本サービスにおいて選択する設定（例：クラスの作成、名簿のインポート、シングルサインオンまたは学習プラットフォーム連携の有効化、クラスの効果測定調査への登録、児童・生徒またはクラスの削除）をいう。その他の指示は、管理者の管理担当者の連絡先が書面で行う。info@eco-heroes.org への電子メールで足りる。

3.3 処理者は、ある指示がGDPR、LOPDGDDその他のEU法または加盟国法のデータ保護規定に違反すると考える場合は、直ちに管理者に通知する。処理者は、管理者が当該指示を確認または変更するまで、その実行を停止することができる。

4. 管理者の義務

4.1 管理者は、処理の適法性（児童・生徒のデータを処理する法的根拠を含む）、GDPR第13条および第14条が求める情報をデータ主体（児童・生徒および、該当する場合はその親または保護者、教師、管理担当者、従業員および宿泊客）に提供すること、デジタル同意年齢に満たない児童・生徒について管理者に適用される法が求める同意を取得すること（GDPR第8条、LOPDGDD第7条：スペインでは14歳）、ならびに管理者およびその利用者が入力するデータの正確性について責任を負う。

4.2 管理者は、その利用者に対し、ニックネーム、クラス名、宿題のメモ、ライブクイズのニックネームおよび調査への回答などの自由記述欄に、特別な種類の個人データ（GDPR第9条）、姓、電子メールアドレスその他の児童・生徒の直接識別子を入力しないよう求める。

4.3 管理者が自らの学習プラットフォーム（LTI）または本人確認プロバイダー（シングルサインオン）を連携させる場合、管理者は、当該システムおよびその設定について責任を負い、附属書Iに記載するデータのみを共有するよう設定する（LTIによる児童・生徒については氏名のみとし、電子メールアドレスは共有しない）。

4.4 管理者は、管理担当者の連絡先を指定し、効果測定調査を実施する前に子どもの保護（セーフガーディング）の担当者を指定し、いずれの連絡先も本サービス内でまたは処理者への電子メールにより最新の状態に保つ。子どもの保護の担当者が指定されるまで、または指定された担当者のアカウントが閉じられている間は、本サービスは子どもの保護に関するフラグを管理者の学校の管理担当者に渡す。本サービス内でいずれの学校にも紐付いていないクラス（LTIによる起動のみで使用されるクラスなど）については、フラグは処理者の子どもの保護責任者に渡され、同責任者はこれを遅滞なく管理者の管理担当者の連絡先に伝える。

5. 処理者の義務

処理者は、次の各号を行う。

a. 第3条に従ってのみ管理者データを処理する。

b. 管理者データの処理を認められた者が守秘義務を負うことを約束し、または適切な法定の守秘義務に服することを確保し、本番システムへのアクセスをそれを必要とする特定の者に限定する。

c. **附属書II**の技術的および組織的措置を講じ、データ主体に子どもが含まれることを考慮して、GDPR第32条に従いリスクに適したセキュリティの水準を維持する。

d. 第6条の条件に従ってのみ他の処理者を使用する。

e. 処理の性質を考慮し、可能な限り、適切な技術的および組織的措置により、データ主体の権利行使の請求（GDPR第12条から第23条）に応じる管理者の義務の履行を、第8条に定めるとおり支援する。

f. 処理の性質および処理者が入手可能な情報を考慮し、GDPR第32条から第36条（セキュリティ、侵害の通知、データ保護影響評価、事前協議）の遵守の確保について管理者を支援する。処理者の現行のデータ保護影響評価の概要はトラストセンターに掲載しており、完全な評価は請求に応じて管理者に提供する。

g. 本サービスの終了時に、管理者の選択に従いすべての管理者データを削除または返還し、EU法または加盟国法がデータの保存を義務付ける場合を除き、既存の複製を削除する（第10条）。

h. GDPR第28条の遵守を証明するために必要なすべての情報を管理者に提供し、管理者または管理者が委任した監査人が行う監査（検査を含む）を受け入れ、これに協力する（第11条）。

i. 管理者に代わって行うすべての種類の処理活動の記録を保持する（GDPR第30条第2項）。

j. 第7条の条件に従ってのみ管理者データを第三国に移転する。

6. 再委託先

6.1 管理者は、**附属書III第A部**に掲げる再委託先について、一般的な書面による承認を与える。

6.2 処理者は、再委託先の追加または交替を予定する場合、少なくとも**30日**前までに、管理者の管理担当者の連絡先への電子メールおよび https://eco-heroes.org/trust/ の更新により、管理者に通知する。管理者は、データ保護に関する合理的な理由に基づき異議を述べることができる。通知期間内に異議が解決されない場合、管理者は、違約金なしに本ライセンスの該当部分を解約することができ、この場合は第10条が適用される。

6.3 処理者は、各再委託先を、当該プロバイダーの標準的なデータ処理条件に基づいて使用する。これらの条件は、GDPR第28条第4項が求めるとおり、適切な技術的および組織的措置について十分な保証を与えるデータ保護義務を再委託先に課すものである。処理者は、各再委託先がこれらの義務を履行することについて、管理者に対して全面的に責任を負う。

6.4 **附属書III第B部**は、処理者が使用するが管理者データを**処理しない**第三者サービスを掲げる。これらは個人データを処理しないか、処理者自身が管理者となるデータのみを処理する。透明性のために掲げるものであり、本契約にいう再委託先ではない。

6.5 管理者自身のシステム（学習プラットフォーム、GoogleまたはMicrosoftの環境など）は、管理者が選択し管理するものであり、処理者の再委託先ではない。

7. 国際移転

7.1 管理者データは欧州連合内でホスティングおよび保存される。アプリケーションサーバーはフランス（Internet Girona、OVHcloudのインフラ上）、データベース、暗号化されたバックアップおよび予備サーバーはドイツとフィンランド（Hetzner Online GmbH）にある。コンテンツ配信ネットワーク（Cloudflare）は、キャッシュされた公開ページをそのグローバルネットワークから配信する。個人データを含む応答は、プライベートかつ保存不可（no-store）として指定されており、同ネットワークはこれをキャッシュしない。

7.2 処理者は、次のいずれかの場合を除き、管理者データを欧州経済領域外に移転せず、またいかなる再委託先にも移転させない。(i) 移転先について欧州委員会の十分性認定がある場合（スイス、および処理者が公式リストで認証を確認した組織についてはEU・米国データプライバシー・フレームワークを含む）、または (ii) 欧州委員会実施決定（EU）2021/914により採択された標準契約条項（モジュール3：処理者から処理者へ、または該当する場合はモジュール2）に基づく場合であって、移転影響評価により必要と判断されたときは補完的措置を講じる場合。附属書IIIに、各再委託先に適用される保護措置を示す。処理者は、欧州経済領域外の各再委託先について書面による移転影響評価を保持し、請求に応じて管理者に提供する。

7.3 Cloudflare, Inc.は、暗号化された接続をそのネットワークのエッジで終端するため、そこでリクエストデータ（IPアドレス、要求されたアドレス、ヘッダー）を処理する。処理者は、標準契約条項を含むCloudflareの標準的なデータ処理条件、およびCloudflareがデータプライバシー・フレームワークの公式リストに掲載されている場合はEU・米国データプライバシー・フレームワークに依拠する。

7.4 Proton AGは、処理者の電子メールをスイスでホスティングする。スイスについては欧州委員会の十分性認定がある。

8. データ主体の権利に関する支援

8.1 教師は、本サービス内で直接、児童・生徒のデータを閲覧し、エクスポート（CSV）し、名前を変更し、リセットし、削除することができ、クラス全体を削除することができる。各教師は自分のクラスのみを閲覧でき、学校の管理担当者は自校のすべてのクラスを閲覧でき、教師のアクセスを直ちに取り消すことができる。管理者は、可能な場合はこれらの機能を用いて請求に応じる。

8.2 請求に本サービスを通じて応じることができない場合、処理者は、書面による請求から**10営業日**以内に管理者を支援する。処理者がデータ主体（親または保護者を含む）から管理者データに関する請求を直接受けた場合、処理者は、その請求の内容には回答しない。処理者は、管理者が別段の指示をしない限り、不当な遅滞なくデータ主体を管理者に案内し、管理者に通知する。

9. 個人データ侵害

9.1 処理者は、管理者データに影響する個人データ侵害を認識した後、不当な遅滞なく、遅くとも**48時間**以内に管理者に通知する。最初の通知には、その時点で判明している範囲で、GDPR第33条第3項が求める情報（侵害の性質、影響を受けるデータ主体および記録の種類およびおおよその数、生じうる結果、ならびに講じたまたは講じる予定の措置）を含める。処理者は、情報が判明するに従い段階的に補足する。

9.2 処理者は、侵害の調査、封じ込めおよび記録について管理者と協力し、監督機関（スペインではAgencia Española de Protección de Datos）への通知およびデータ主体への連絡について管理者を支援する。処理者は、事実関係、影響および講じた是正措置を含め、すべての個人データ侵害を記録する。

9.3 処理者は、管理者の管理担当者の連絡先に電子メールで通知を送付する。何人も、セキュリティ上の脆弱性を security@eco-heroes.org に報告することができる。報告は5営業日以内に受領確認され、重大な問題は他のすべての作業に優先して修正される。

10. 保存、削除および返還

10.1 **本ライセンスの期間中。**管理者データは、本サービスのコードに実装された保存規則を反映した附属書I第C節の計画に従って保存される。教師は、いつでも児童・生徒またはクラスを削除することができ、その削除は稼働中のデータベースおよび予備のレプリカに即時に反映される。

10.2 **エクスポート。**本ライセンスの期間中および第10.3条による削除までの間、管理者は、本サービス内でクラスおよび進捗のデータをCSVとしてエクスポートし、または構造化され、一般的に使用され、機械可読な形式でのエクスポートを処理者に請求することができる。

10.3 **本ライセンスの終了。**本ライセンスが終了し更新されない場合、処理者は、終了日から**90日**後に管理者データを削除する。管理者が書面で請求した場合、処理者は、本ライセンスが終了したか否かにかかわらず、請求から**30日**以内に管理者データを削除する。処理者は、請求に応じて削除を書面で確認する。削除に先立ち、処理者は、削除日の30日前および7日前に、管理者の学校管理担当者に対し、当該日付ならびに本ライセンスの更新方法およびデータのエクスポート方法を記載した電子メールを送信する。削除は、1通目の送信から30日、2通目の送信から7日が経過するまで行わない。

10.4 **教師アカウント。**教師アカウントに紐付く最後のライセンスが終了した場合、当該アカウントは無料の教師アカウントとして存続する。当該アカウントは、その間に教師が新たなライセンスに紐付けられない限り、そのライセンスの終了から12か月後に削除される。無料アカウントは、ログインのない状態が12か月続いた後に削除される。処理者は、削除の30日前に教師に電子メールを送付する。教師アカウントが存続しても、管理者データが保持されることを意味しない。管理者データは第10.3条に従い削除される。

10.5 **バックアップおよびレプリカ。**削除されたデータは、通常のサイクルでバックアップから消える。暗号化されたバックアップはローテーションで保持されるため、削除されたデータは**14日**以内にすべてのバックアップから消える。予備サーバーの読み取り専用レプリカは、すべての削除を継続的に反映する。バックアップは本番システムの損失を回復するためにのみ復元され、復元により削除済みのデータが再現された場合は、削除が再度適用される。

10.6 **法定の保存。**処理者は、本ライセンスの終了後は、EU法または加盟国法が求める範囲および期間に限り個人データを保存する。例えば、スペイン商法典（Código de Comercio）第30条に基づき請求書および会計記録を6年間保存する。これらの記録は管理者の連絡担当者を特定するものであり、児童・生徒のデータを含まない。処理者は、これらを附属書IIに従って保護し、他の目的には使用しない。

11. 監査および情報

11.1 処理者は、請求に応じ、契約年度ごとに1回を上限として（ただし、個人データ侵害の後、または不遵守についての文書化された合理的な疑いがある場合は追加で）、本契約の遵守を証明するために必要な情報を管理者に提供する。これには、現行のセキュリティ概要（https://eco-heroes.org/trust/#security）、現行の再委託先リスト、管理者に代わって行う処理の記録、移転影響評価、データ保護影響評価、直近の復元テストおよびフェイルオーバー訓練の結果、ならびに実施したセキュリティレビューの結果が含まれる。

11.2 これらの情報が十分でない場合、管理者、または管理者が委任し守秘義務を負う独立の監査人は、少なくとも**30日**前の通知により、通常の営業時間内に、処理者の業務または他の顧客を不当に妨げることなく、処理者の関連する処理を監査することができる。各当事者は自らの費用を負担する。処理者は、監査人に合理的な秘密保持契約への署名を求め、他

の顧客と共有するシステムへのアクセスを遵守の確認に必要な範囲に限定することができる。

12. 責任

12.1 各当事者は、GDPR第82条に従いデータ主体に対して責任を負う。当事者間においては、責任は本ライセンスの責任条項による。本契約または本ライセンスのいかなる規定も、法が制限を認めない場合（故意による責任を含む）に、当事者の責任を制限するものではない。

12.2 処理者が、管理者の指示により、または管理者が第4条の義務を履行しなかったことにより、行政上の制裁金または損害賠償を支払わなければならない場合、管理者は、その原因の範囲で処理者を補償する。その逆も同様とする。

13. 期間、準拠法および裁判管轄

13.1 本契約は、本ライセンスの開始日に効力を生じ、第10条に従いすべての管理者データが削除または返還された時に終了する。第5条(b)、第10条、第11条および第12条は、必要な期間効力を存続する。

13.2 本契約は、スペイン法ならびにGDPRおよびLOPDGDDを含むEU法に準拠する。Girona（スペイン）の裁判所が管轄権を有する。ただし、管理者が公的機関として、または公共調達法に基づき適用を受ける強行規定、およびGDPR第79条に基づくデータ主体の権利を妨げない。附属書Vに、英国および米国の管理者に関する規定を追加する。

13.3 本契約の変更は書面で行う。電子メールで足りる。処理者は、現行のひな形を https://eco-heroes.org/trust/ に掲載する。ひな形の新しい版は、管理者の同意なく、署名済みの本契約を変更しない。管理者の学校の管理担当者は、本契約をオンラインで承諾することができる。処理者は、誰が、いつ、どの版を承諾したか、および使用されたIPアドレスの鍵付きハッシュを記録する。

署名

管理者のために	処理者のために — Eco Heroes International SL
氏名、役職	Karim Zouhdi、創業者
日付、署名	日付、署名

附属書I — 処理の詳細

A. 管理者に代わって行う処理（本契約の対象）

附属書I.A — 管理者に代わって行う処理

項目	内容
対象事項	本ライセンスに基づく、管理者の利用者に対する本サービスの提供。
性質	データのホスティング、保存、表示および削除、進捗の記録、クラスでのライブクイズ、宿題、修了証、クラス管理、管理者が提供する名簿の任意のインポート（貼り付けまたはCSVのアップロード、OneRoster CSV 1.1/1.2、Google Classroom）、管理者の学習プラットフォームからの任意のLTI 1.1／LTI 1.3起動（Names and Role Provisioning（名簿のインポート）およびAssignment and Grade Services（得点の返送）を含む）、管理者の選択によるGoogleまたはMicrosoftでの任意の教師ログイン、管理者がクラスコードを配布する場合のEco Heroesモバイルアプリのクラスダッシュボード、管理者が登録したクラスにおける任意の効果測定調査の質問票、企業およびホテル向けライセンスにおけるコーディネーターアカウント、グループのアクセスコードおよびグループごとの進捗レポート（CSV）、サポート。企業およびホテルのライセンスでは、さらに：組織向けの集計された活動レポート（組織レポートおよび合計値。5家族未満にもとづく数値は非表示）と任意のチームランキング、子どもの修了証への組織名とロゴの表示、管理者自身のIDプロバイダーによるスタッフの任意のサインイン（OpenID Connect）。
目的	国連の持続可能な開発目標に基づく持続可能性教育を、本ライセンスが定める進捗の記録、報告および評価とともに提供すること。効果測定調査については、管理者自身の授業の評価（管理者の教師向けのクラス結果）および第2.3条による匿名化された集計統計。その他の目的はない。
データ主体の種類	児童・生徒（ゲームは9歳から17歳を対象とし、9〜12歳と13〜17歳の2つの年齢グループがある。印刷用の授業シートは6歳から16歳を対象とし、管理者はその裁量により、より年少の児童に本サービスを使用することができる）、教師、学校の管理担当者、同意手続が使用される場合に限り親および保護者、企業およびホテル向けライセンスにおいては従業員または宿泊客の子どもおよび組織のコーディネーター。
個人データ — 児童・生徒（ウェブサイト、クラス内）	児童・生徒または教師が入力する名またはニックネーム（2〜24文字。名簿インポートでは名と姓の頭文字とし、同じ名の2人を区別する場合に限り姓の最初の3文字までに拡張する。氏名全体は使用しない）、ゲーム内で選択した年齢グループ（9〜12歳または13〜17歳）、固定のセットから選ぶアバター、言語、進捗（ポイント、達成した目標およびミッション、クイズの星、テーマごとの回答数および正答数）、完了した宿題、参加日および最終活動日、進捗を保存するために児童・生徒の端末に保存されるランダムなクラストークン。クラスでのライブクイズでは、入力されたニックネーム、回答、回答時間および得点。収集しないもの：電子メールアドレス、姓、写真、生年月日、住所、位置情報、端末識別子または広告識別子。

項目	内容
個人データ — 児童・生徒（LTI起動）	プラットフォームのユーザー識別子の鍵付きハッシュ（児童・生徒を席に紐付けるため）、プラットフォームが成績サービスへのアクセスを付与した場合に限り起動記録に90日間保存されるプラットフォームのユーザー識別子（得点の返送に必要）、ニックネームとしての名および姓の頭文字、コース識別子およびコース名、役割、ロケール、直近に送信した得点。電子メールアドレスおよび氏名全体は保存しない。管理者は、氏名のみを共有するよう自らのプラットフォームを設定する。
個人データ — 児童・生徒（モバイルアプリ、クラスダッシュボード）	活動（プレイした日替わりゲーム、日付、言語、得点、完了、所要時間、達成した目標、バッジ）、およびアプリが生成するランダムなインストール識別子の一方向ハッシュ。児童・生徒は、生成された別名で教師に表示される。ダッシュボードは、活動中の児童・生徒が5人未満のクラスについては何も表示しない。
個人データ — 児童・生徒（管理者がクラスを登録した場合の効果測定調査）	調査の質問票への回答（選択、評価および任意の短い自由記述）、質問票の版、言語、年齢グループ、開始および送信の時刻、ならびに品質の指標。電子メールアドレスおよび電話番号は、受信時に自由記述から削除される。子どもの保護に関わる打ち明けを含むおそれのある回答は、管理者が指定した担当者に知らされる。回答は、クラス内の児童・生徒の席の鍵付き一方向ハッシュにより調査の各回の間で紐付けられ、氏名、電子メールアドレスおよび生年月日は収集しない。席ごとに、管理者が記録した異議または書面による同意。子どもの保護の担当者が指定されていない場合は、第4.4条に定める受領者がこれに代わる。
個人データ — 教師および学校の管理担当者	氏名、業務用電子メールアドレス、学校、役割（教師または学校の管理担当者）、言語、パスワード（bcryptハッシュ）またはシングルサインオンの識別子、有効な場合は二段階認証の秘密鍵およびハッシュ化されたバックアップコード（学校の管理担当者は必須）、電子メールの確認状態、ログインの時刻および回数、セッション、作成したクラス、名簿インポートのプレビュー（氏名のみ、セッション内に30分間保持）、管理操作の監査ログの記録（IPアドレスの鍵付きハッシュ、およびコンテンツ配信ネットワークから得る接続元の国の2文字コードを含む）、サポートのやり取り。
個人データ — 教師（効果測定調査）	教師用質問票への回答、および6〜8歳の児童についてはクラスの観察シート。教師のアカウントまたはコードの鍵付き一方向ハッシュにより紐付けられる。クラスの登録、その同意の形式および調査におけるグループへの割当て。
個人データ — 親および保護者	デジタル同意年齢に満たない児童・生徒についてウェブサイトの保護者同意手続が使用される場合に限り、親の電子メールアドレスの鍵付き一方向ハッシュ（アドレスそのものは確認リンクの送信に1回使用し、保存しない）、判断およびそのタイムスタンプ。

項目	内容
個人データ — 子どもおよびコーディネーター（企業およびホテル向けライセンス）	管理者の従業員または宿泊客の子ども：自分の端末または家族の端末で、管理者のアクセスコードとヒーロー名（ニックネーム）によりグループに参加し、アカウントも電子メールアドレスも持たない。本サービスは、クラスの児童・生徒と同じデータ（ヒーロー名、年齢グループ、アバター、言語、進捗およびクイズの結果）を保存する。コーディネーター：氏名、業務用電子メールアドレス、パスワードハッシュまたはログイン識別子、二段階認証の設定、および作成したグループ。コーディネーターは、グループごとに達成した目標およびクイズの結果を閲覧し、CSVとしてエクスポートすることができる。組織レポートのため、本サービスはこれらのグループの各ヒーロープロフィールについて、活動した日と、各目標・各ミッションを初めて達成した日も記録する（日単位。学校のクラスについてはこの記録を行わない）。レポートには集計値のみが含まれ、名前、ニックネーム、識別子、子どもごとの行は含まれない。1〜4家族にもとづく数値は非表示とし（k = 5）、ひとつの数値だけでそれが推測できる場合には、もうひとつの数値も非表示とする。チーム名は管理者の管理担当者が選び、個人の名前を用いてはならない。管理者が企業アカウントでのサインインを有効にした場合、スタッフの氏名とメールアドレスは管理者自身のIDプロバイダー（スコープ openid、email、profile）から取得する。このIDプロバイダーは管理者自身のシステムかつ管理者自身の処理者であって再委託先ではなく、そのサブジェクト識別子は鍵付きハッシュとしてのみ保存する。共同ブランド表示：管理者が提供する組織の表示名とロゴ。保護者がLinkedIn で共有できる公開バッジページには個人データは含まれない（目標の数、管理者がオプトインした場合の組織名、言語のみで、いずれもリンクから取得する）。共有は大人が開始し、処理者は LinkedIn に何も送信しない。
特別な種類（GDPR第9条）	求めておらず、必要もない。第4.2条を参照。
頻度	本ライセンスの期間中、継続的に。

B. Eco Heroesが独立した管理者として行う処理（本契約の対象外）

本契約の範囲を管理者が確認できるよう掲げる。これらは処理者のプライバシーポリシー（v4.3）および子どものプライバシーに関する通知（v2.2）の対象であり、本契約の対象ではない。

- **教師アカウントそのもの：** ログイン、セキュリティ、二段階認証および無料の教師向け教材。処理者はアカウントそのものの管理者であり、第10.4条に従って削除する。管理者のためのアカウントの活動は管理者データである。
- **無料の教師アカウント：** ライセンスに紐付けられていない教師で、確認済みの電子メールアドレスにより無料の教師向け教材（ハンドブックの授業および教師用ガイド）を利用する者。
- **ファミリープラン**（ウェブサイト上で親または保護者が契約するもの）：電子メールアドレス（一部をマスクして保存）、Stripeの支払いおよびサブスクリプションの参照情報、ならびに個人のアクセスコード（鍵付きハッシュとして保存）。カード情報は処理者に届かない。学校で使用されるファミリーコードは、学校のデータを一切伴わない。
- **アプリのアカウント**（GoogleまたはAppleによる保護者のログイン、Google PlayまたはAppleによるサブスクリプション、RevenueCatによるサブスクリプションの状態）。
- **ウェブサイトの訪問者**（大人向けの公開ページ：同意後のGoogle Analytics 4、Formspreeによるお問い合わせフォーム、処理者自身のサーバーによる見積依頼およびアンバサダー応

募、BrevoによるDinner Questionsメール）。

- **クイズの公開ランキング**（任意：生成されたリストから選ぶニックネーム、得点およびIPアドレスの鍵付きハッシュ。30日間保存）。
- **プログラム調査：** 処理者がクラス外で実施するもの。法が求める場合は親の同意を得る。
- **別個のサービス：** Eco Heroes Academy（learn.eco-heroes.org）およびVSME評価（assessment.eco-heroes.org）は、独自の規約およびプライバシーに関する情報を有する。

C. 保存計画（本サービスに実装されているもの）

附属書I.C — 保存計画

データ	保存	仕組み
児童・生徒のデータならびに企業およびホテルのグループの子どものデータ（ニックネーム、年齢グループ、アバター、進捗、宿題、アプリのクラス活動、LTIの席の紐付け）	本ライセンスの期間中：教師または管理担当者が児童・生徒またはクラスを削除するまで。本ライセンスの終了後：本ライセンスが更新されない限り、終了日から90日後に削除。管理者の書面による請求があった場合：30日以内に削除。削除の30日前および7日前に学校管理担当者へ電子メールで通知	本サービス内での教師または管理担当者の操作、ライセンス終了時の自動削除、書面による請求に基づく処理者の対応
企業およびホテルのグループに属するヒーロープロフィールの活動日（組織レポート）	ヒーロープロフィールとともに保存し、上記の規則に従ってプロフィールと一緒に削除	プロフィールとともに削除
組織の設定：チーム名と各グループのチーム割り当て、チームランキングの設定、共同ブランド表示の名前とロゴ、企業アカウントでのサインインの設定	ライセンス期間中。管理者の依頼により削除	依頼に応じて処理者が実施
企業アカウントでのサインイン：サインイン手続きの記録、固定されたID連携（IDプロバイダーのサブジェクトの鍵付きハッシュ）	手続きの記録：使用時または10分後に削除。ID連携：アカウントが削除されるか、管理者のサインイン設定が削除またはリセットされるまで	自動削除、管理担当者による操作
クラスでのライブクイズ（ニックネーム、回答、時間、得点）	クイズセッションの作成から30日	日次の自動消去
名簿インポートのプレビュー（OneRoster）	30分、教師のサーバーセッション内のみ	セッションの期限切れ
Google Classroomのアクセストークン（名簿インポート）	インポート中のみ、教師のセッション内。データベースには書き込まない	セッションの期限切れ
LTI起動記録	教師の起動および成績サービスのない児童・生徒の起動：2時間。成績サービスのある児童・生徒の起動：90日	LTI活動時の自動消去
LTIのログイン状態、引継ぎトークン、ディープリンクトークン、ノンス、名簿インポートトークン	10分／10分／60分／15分／2時間	自動消去、1回限りの使用

データ	保存	仕組み
教師、コーディネーターおよび学校の管理担当者のアカウント	アカウントに紐付く最後のライセンスの終了から12か月。無料アカウントはログインのない状態が12か月続いた後。削除の30日前に警告メール。未確認の登録：最後の確認リンクの期限切れから7日後に削除	アカウントの自動消去
セッションおよび「ログイン状態を保持」	設定された期間のサーバーセッション。ログイン時および30分ごとに更新。パスワードの変更時または管理担当者がアクセスを取り消した時にすべてのセッションが終了。「ログイン状態を保持」Cookie：180日（HMAC署名付き）	コード
レート制限の記録（ログイン試行その他の制限）	30日	日次の自動消去
セキュリティ監査ログ（管理操作、コードの有効化、ログイン。IPの鍵付きハッシュ、接続元の国の2文字コード）	12か月	日次の自動消去
調査への回答および同意依頼における不正防止用のIPハッシュ	30日（回答そのものは独自の期間に従う）	日次の自動消去
保護者同意の依頼	未回答または期限切れ：30日。拒否：12か月。与えられた同意：依拠する間。同意が撤回された場合はデータとともに削除	日次の自動消去、削除機能
効果測定調査の回答（児童・生徒、教師、観察シート）ならびに異議または同意の記録	調査の最終回の終了から24か月。管理者の書面による指示があればそれより早く。異議および同意の記録はクラスの登録とともに削除	日次の自動消去、書面による請求に基づく処理者の対応
子どもの保護に関するフラグ（打ち明けを含むおそれのある効果測定調査の回答、およびそれが属する席とニックネーム）	回答の本文は、フラグが対応済みとされてから30日後に消去し、フラグの記録は対応から12か月後に削除する	日次の自動消去
プログラム調査への回答	24か月、または同意が撤回されるまで	日次の自動消去、削除機能
クイズの公開ランキングの記録（本契約の対象外、完全性のために掲載）	30日	日次の自動消去
管理者による本契約の承諾の記録（承諾した者、日時、バージョン、IPアドレスの鍵付きハッシュ。処理者が管理者として保持する。第13.3条）	ライセンスの期間中およびその終了後6年	処理者の記録
ファミリープランの支払い時の同意、解約および撤回の記録（本契約の対象外、完全性のために掲載）	会計記録とともに6年（スペイン商法典第30条）	会計記録
個人から導出される参加率のカウンター	2日	日次の自動消去

データ	保存	仕組み
テレメトリー（CSP違反およびJavaScriptエラーの報告）	識別子は保存しない（短縮したユーザーエージェント）。レートカウンターは1分ごとにリセット。ログの上限は5 MB	コード
サポートのやり取り（電子メール）	請求が処理されるまで、かつ最後のメッセージから最長12か月	処理者のメールボックスの手順
暗号化されたバックアップ	暗号化されたバックアップはローテーションで保持。削除されたデータは14日以内にすべてのバックアップから消える	自動
データベースの予備レプリカ	継続的。すべての削除を反映	レプリケーション
ウェブサーバーの技術ログ（IPアドレス、要求されたアドレス）	最長90日	サーバー設定
請求書および支払記録	6年（スペイン商法典第30条）。管理者の連絡担当者を特定するものであり、児童・生徒を特定するものではない	会計記録

附属書II — 技術的および組織的措置（GDPR第32条）

本契約の日付時点で有効な措置。各リリース時に見直され、現行の概要は https://eco-heroes.org/trust/#security に掲載される。処理者は、全体としてのセキュリティの水準が低下しない限り、措置を更新することができる。

1. 通信中の暗号化

- すべての接続にTLS 1.2以上を使用。HTTP Strict Transport Security（max-age 2年、includeSubDomainsおよびpreload）。証明書の自動更新。コンテンツ配信ネットワークとサーバーの間はオリジン証明書を使用。
- アプリケーションサーバーは、固定した認証局に対して証明書を検証するTLS 1.2/1.3によってのみデータベースに接続する。データベースは暗号化されていない接続を拒否する（require_secure_transport）。データベースのアカウントは、アプリケーションホストおよび予備ホストに限定される。
- バックアップは、サーバーを離れる前に暗号化され（AES-256-CBC、20万回反復のPBKDF2）、暗号化された接続でのみ送信される。暗号化されていないアーカイブは書き込まれない。

2. ブラウザにおける保護

- Content-Security-Policy：インラインスクリプトは、スクリプトごとのSHA-256ハッシュで承認されたもの、または一部の動的ページではリクエストごとのノンスを持つものに限り実行される（スクリプトにunsafe-inlineは使用しない。インラインスタイルは引き続き許可。object-src 'none'、base-uri 'self'、frame-ancestors 'none'。ただし、登録された学習プラットフォームのみが埋め込めるLTIページを除く）。違反の報告はレート制限付きで収集される。子ども向けページは第三者のスクリプトを読み込まない。大人向けページにおける第三者のスクリプトは、同意後のGoogle Analytics、ならびにログインおよび登録フォームにおけるCloudflare Turnstileの確認に限られる。
- ウェブフォントは処理者自身のサーバーでホスティングされる。Google Fontsその他のフォントプロバイダーへのリクエストは送信されない。
- セキュリティヘッダー：X-Content-Type-Options: nosniff、X-Frame-Options: DENY、Referrer-Policy、Permissions-Policy、Cross-Origin-Opener-PolicyおよびCross-Origin-Resource-Policy same-origin。サーバーおよびPHPのバージョンヘッダーは削除される。HTTP TRACEおよびTRACKは拒否される。
- Cookie：セッションCookieはSecure、HttpOnlyおよびSameSite=Strictで、厳格セッションモードを使用する。セッションIDは、ログイン時、コードの有効化時および30分ごとに変更される。「ログイン状態を保持」Cookieはサーバーサイドのキーで HMAC署名される。LTIの状態Cookieは/lti/に限定され、パーティション化される。
- ゲームのサービスワーカーは、no-storeまたはprivateと指定された応答、および会員限定のパスを決してキャッシュしないため、共有端末でログアウトした後に保護されたコンテンツがキャッシュに残らない。
- 個人データまたは会員限定コンテンツを含む応答はCache-Control: private, no-storeで送信され、コンテンツ配信ネットワークはこれを決してキャッシュしない。

3. アクセス制御および認証

- 本人名義の教師アカウント：学校コードは登録のために1回だけ使用される。学校コードは、確認済みの電子メールアドレスを持つ本人名義のアカウントを作成するか、教師の既存のアカウントに学校を紐付ける。その後、教師は自分の電子メールアドレスとパスワードで、またはシングルサインオンでログインする。学校コードのみが入力された端末は、ゲームをプレイすることはできるが、教師用ツールは使用できない。管理者コードは学校の最初の管理担当者アカウントのみを作成し、当該アカウントの確認をもって使用済みとなる。その後、教師は、学校管理担当者が本サービス上で作成する教職員コードにより参加する。教職員コードは1回だけ表示され、鍵付きハッシュとしてのみ保存され、いつでも差し替えることができる。
- 教師のパスワードはbcryptでハッシュ化され、一定時間で比較される。最初のログインの前に電子メールアドレスの確認が必要。パスワードを変更するとすべてのセッションが終了する。学校の管理担当者は、教師のアクセスを直ちに取り消すことができる。
- 二段階認証（ハッシュ化されたバックアップコード付きのTOTP）は、学校の管理担当者および処理者のスーパー管理者に必須であり、すべての教師ならびに企業およびホテルのライセンスのコーディネーターが有効にすることができる。登録用のQRコードはサーバー上で生成されるため、秘密鍵がサーバーの外に出ることはない。第二の要素はセッションが作成される前に確認され、学校の管理担当者は児童・生徒のデータが表示されるあらゆる場所でこれを使用しなければならない。子どもの保護の担当者も、子どもの保護に関するフラグを読むにはこれを使用しなければならない。24時間以内に誤ったコードが10回入力された場合、そのアカウントの第二の要素は15分間ロックされ、アカウントの所有者に電子メールで通知される。
- アクセスコードは、ウェブルートの外にあるファイルに鍵付きハッシュとしてのみ保存される。鍵はウェブルートの外に保管される。登録コードおよびライセンスコードも同様に保存される。コードは作成時に1回だけ表示される。
- ログイン（IPアドレスごと、および電子メールとIPの組合せごとに、全体の上限付き）、登録、コードの引換え、クラスへの参加、ライブクイズへの参加、進捗の同期、見積フォーム、LTIログイン、テレメトリーのエンドポイントおよびStripeの戻り参照にレート制限を適用。データを変更するすべてのフォームにCSRFトークン。すべてのnext=パラメーターにオープンリダイレクト対策。
- アクセス権はサーバーで確認される。会員限定のリソース（ミッション動画、クイズの問題バンク、書籍、LTIコンテンツ）は、サーバーが有効なコードセッション、署名付きの記憶されたコードまたはログイン済みのアカウントを確認した後にのみ配信される。ブラウザ自身が書き込むものによってアクセスが与えられることはない。
- 役割および学校による分離：各教師は自分のクラスのみを閲覧できる。学校の管理担当者は自校のすべてのクラスを閲覧でき、他校のものは一切閲覧できない。LTIで来た教師は、起動元のコースのクラスのみを閲覧できる。スーパー管理者のアクセスは、処理者の特定の職員に限定される。
- すべてのデータベースクエリはプリペアドステートメントを使用する。exec、evalおよびunserializeは使用しない。ファイルパスは許可リストの要素からのみ組み立てる。アップロード（名簿のCSV/ZIPファイル、調査用の画像）は、サイズを制限し、種類を確認し、ウェブルートの外に保存する。PHPエラーの表示は無効にしている。
- 企業およびホテルのスタッフ向けの任意のシングルサインオン（OpenID Connect。Authorization Code と PKCE を使用し、署名付きIDトークンの発行者、対象者、有効期限、nonce を検証）。クライアントシークレットは暗号化して保存する。アカウントの照合は管理

者が許可したメールドメインの範囲内でのみ行い、他の組織のアカウントに結びつけることはない。

4. データの最小化および子どものデータ

- 児童・生徒の電子メールアドレス、姓、写真、生年月日、住所、位置情報、端末識別子または広告識別子は収集しない。名簿インポートでは、名と姓の最初の3文字までのみを保持する。LTIで来た児童・生徒は、プラットフォームのユーザー識別子の鍵付きハッシュと、名および姓の頭文字で保存される。管理者は、氏名のみを共有するよう自らのプラットフォームを設定する。
- IPアドレスは鍵付きハッシュ（プレフィックス）としてのみ保存される。鍵を持つ者はこれらを再び関連付けることができるため、匿名ではなく仮名化されたものである。コンテンツに付随する場合は30日後に削除される。
- 子ども向けページ（/game、/games、/trivia、/library、/sdg、/wordle、/missions、/booksおよびその各言語版）は、分析を読み込まず、同意バナーも表示しない。その他のページでは、明示的な同意の後にのみ分析が読み込まれる。
- 会員限定のミッション動画は処理者がホスティングし、アクセス権を確認した後に配信される。YouTubeプレーヤーが残っている場合（無料プレイ）、youtube-nocookie.comを使用し、利用者が再生を押した時にのみ読み込まれる。
- クイズの公開ランキングへの掲載は、各ゲームの後に任意で選択するものであり、生成されたニックネーム（形容詞と動物。自由記述なし、学校の表示なし）で行われる。公開ランキングは直近30日間の上位10件のニックネームと得点を表示し、記録は30日後に削除される。公開の各行には報告用のリンクがあり、3回報告された行は確認されるまで非表示になる。クラスのランキングは、そのクラスの教師および学校の管理担当者のみが閲覧でき、これらの者は行を削除することができる。
- 自由記述の回答は、送信時に自動的にフィルタリングされる。電子メールアドレスおよび電話番号は削除され、子どもが危険にさらされている可能性を示す語の短いリストに一致する回答は、調査データから取り除かれ、学校が指定した子どもの保護の担当者にのみ渡される。氏名は自動的には削除されない。回答を読む研究者が氏名と思われるものに印を付け、報告書でそれに言及することはない。打ち明けの可能性があるものは、1授業日以内に学校が指定した担当者に渡される。子どもの保護の担当者が指定されていない場合は、第4.4条に定める受領者がこれに代わる。
- 同意手続における親の電子メールアドレスは平文で保存されることはなく、鍵付きハッシュのみが保持される。
- 組織レポートは集計値である。5家族未満にもとづく数値は計算の段階で非表示となるため、画面にも CSV にも表示されない。開けるのは2段階認証でサインインした組織の管理者だけであり、閲覧と書き出しには回数制限があり、すべて記録される。

5. 可用性、バックアップおよび復旧

- 以下は自動的に実行される。独立した監視（UptimeRobot、11項目、5分ごと）が障害時に処理者に警告する。
- データベースとアプリケーションを毎晩暗号化してバックアップし、その写しを別のEU加盟国にある独立したデータセンターに保管する。復元は毎月自動でテストする。
- 各リリースの前にバックアップを取得し、テスト済みのロールバック手順を用意する。以前の本番バージョンは保持される。

- 予備サーバーはアプリケーションの写しとデータベースのライブレプリカを保持する。メインのウェブサーバーに障害が起きた場合は、ヘルスチェック付きの負荷分散が自動的にトラフィックを切り替える。データベースサーバーに障害が起きた場合は、スクリプト化され訓練済みの手順でレプリカを昇格させる。いずれも2026年10月にテスト済みである。
- 1時間ごとのインフラ確認（レプリカの状態および遅延、証明書の有効期限、ディスク容量、保留中のセキュリティ更新、コンテンツ配信ネットワークのアドレス範囲）。オペレーティングシステムのセキュリティ更新は自動的に適用される。ネットワークのエッジでDDoS攻撃およびボットから保護。
- テスト環境は本番から分離されている（別のUnixユーザー、open_basedir付きのPHPプール、別のデータベースインスタンス、秘密情報は削除）。

6. ログ記録および監視

- セキュリティイベント（失敗したログイン、コードの引換え、管理操作、CSP違反の報告、保存期間に基づく削除および消去）は、IPアドレスの鍵付きハッシュとともに記録される。セキュリティ監査ログは12か月、レート制限の記録は30日間保持される（附属書I第C節）。
- 本サービスの現在の状態および各障害は、公開のステータスページに掲載される。

7. 組織的措置

- 本番システムへのアクセスは特定の者に限定される。すべての管理用アカウント（ホスティング、データベースおよびバックアップのサーバー、コンテンツ配信ネットワークおよびDNS、ソースコードリポジトリ、監視、電子メール）は二段階認証を使用する。サーバーへのアクセスはSSH鍵で行う。ファイアウォールは、データベースおよび予備サーバーへのアクセスを、処理者自身のホストおよびコンテンツ配信ネットワークのアドレス範囲に限定する。
- 変更は自動的にテストされ（継続的インテグレーション。テストに合格しないコードのリリースは拒否される）、まずテスト環境を経由し、各リリース後に本番で確認される（47項目のライブチェック）。アプリケーションの静的セキュリティレビューを実施し、記録している（直近：2026年10月16日）。
- ペネトレーションテスト（2026年10月）：処理者自身のテストチームが、プラットフォームを対象にホワイトボックスおよびグレーボックスの体系的なテストを実施した（認証、セッション、学校間のアクセス制御、決済、ファイルとデータの露出、レート制限、エッジキャッシュ）。重大・高・中の指摘事項はすべてリリース前に修正し、再テストした。独立した企業による外部ペネトレーションテストを予定している。
- 脆弱性報告の窓口を/.well-known/security.txtに掲載している。報告は5営業日以内に受領確認され、重大な問題は他のすべての作業に優先して修正される。
- インシデント対応の書面による手順は、処理者が個人データ侵害をどのように検知し、封じ込め、記録するか、および第9条の48時間の通知期限をどのように遵守するかを定める。
- 処理者は、管理者に代わって行う処理の記録（GDPR第30条第2項）、および欧州経済領域外の各再委託先についての移転影響評価を保持する。
- 保存期間はそれを適用するコードの中で定められており、公表された期間と適用される期間が食い違うことはない。
- 秘密情報（制限付きStripeキー、シングルサインオンの認証情報、ハッシュの鍵）はウェブルートの外に保管され、ソースコードリポジトリに入れられることはない。

附属書III — 再委託先および第三者サービス

トラストセンター（https://eco-heroes.org/trust/#subprocessors）に同じ2つのリストを掲載している。

第A部 — 管理者データを処理する再委託先

附属書III.A — 承認された再委託先

再委託先	業務内容	所在地	移転の保護措置
Internet Girona（OVHcloudのインフラ上）	ウェブホスティング	フランス（EU）	EU内。プロバイダーの標準的なデータ処理条件
Hetzner Online GmbH、Gunzenhausen（ドイツ）	データベースのホスティング、予備サーバー、暗号化されたバックアップ	ドイツおよびフィンランド（EU）	EU内。Hetznerの標準的なデータ処理条件
Cloudflare, Inc.、サンフランシスコ（米国）	コンテンツ配信、TLS、攻撃およびボットからの保護、ログインおよび登録フォームにおけるTurnstileの確認、障害時の自動切替え	グローバルなエッジネットワーク。オリジンサーバーはEU内	標準契約条項（2021/914）を含むCloudflareの標準的なデータ処理条件。Cloudflareがリストに掲載されている場合はEU・米国データプライバシー・フレームワーク
Proton AG、ジュネーブ（スイス）	info@およびsecurity@eco-heroes.orgの電子メールのホスティング：管理者の職員とのサポートおよびデータ保護に関するやり取り	スイス	スイスに関する欧州委員会の十分性認定。Protonの標準的なデータ処理条件
Google（Google Ireland Ltd／Google LLC）— ログインおよびClassroomのインポートのみ	管理者が有効にした場合のみ：教師のログイン（氏名、電子メールアドレス、識別子。児童・生徒のデータなし）、Google Classroomからの名簿インポート（姓名を1回読み取り、名と姓の頭文字として保存。アクセストークンは教師のセッション内にとどまる）	EU／米国	管理者自身のGoogleの規約。標準契約条項を含むGoogleの標準的なデータ処理条件。リストに掲載されている場合はEU・米国データプライバシー・フレームワーク
Microsoft（Microsoft Ireland Operations Ltd）— ログインのみ	管理者が有効にした場合のみ：教師のログイン（本人確認のみ。児童・生徒のデータなし）	EU／米国	管理者自身のMicrosoftの規約。標準契約条項を含むMicrosoft Products and Services DPA。リストに掲載されている場合はEU・米国データプライバシー・フレームワーク

再委託先	業務内容	所在地	移転の保護措置
Google（YouTube、youtube-nocookie.com）	YouTubeプレーヤーが引き続き使用されている一部の教育動画の再生：プライバシー強化モード、利用者が再生を押した時にのみ読み込み	EU／米国	Googleの規約。リストに掲載されている場合はEU・米国データプライバシー・フレームワーク
Moodle Pty Ltd（MoodleCloud）、西オーストラリア	管理者が自らの学習プラットフォームの代わりにEco Heroesのコースサイトeco-heroes.moodlecloud.comを使用する場合のみ：そのサイトのコースアカウント、およびゲームがそこに報告する進捗	Amazon Web Services上のMoodleCloudのホスティング	欧州経済領域外へのあらゆる移転について標準契約条項（2021/914）を含むMoodleCloudのデータ処理契約

第B部 — 管理者データを処理しない第三者サービス

透明性のために掲げる。個人データが関わる場合は、処理者のプライバシーポリシーが適用される。アカウント、確認およびサービスに関する電子メールは処理者自身のメールサーバーが送信し、これは第三者ではない。

附属書III.B — 本契約の対象外の第三者サービス

サービス	業務内容	所在地	本契約の対象外である理由
Stripe	ウェブサイトにおけるファミリーサブスクリプションのカード決済。処理者は支払いおよびサブスクリプションの状態を読み取る	EU／米国。標準契約条項を含むStripeのデータ処理条件。EU・米国データプライバシー・フレームワーク	ファミリー会員は処理者自身の顧客であり、学校のデータはStripeに送られない
Google Analytics 4	大人向けの公開ページにおける訪問統計。同意後のみ。子ども向けページおよび教師エリアでは使用しない	EU／米国。標準契約条項を含むGoogleのデータ処理条件。EU・米国データプライバシー・フレームワーク	管理者データは送られない。処理者は自らのウェブ統計の管理者である
Formspree	一般のお問い合わせフォームからのメッセージを転送	米国。プロバイダーの標準的なデータ処理条件（標準契約条項。リストに掲載されている場合はEU・米国データプライバシー・フレームワーク）	メッセージは処理者自身のやり取りであり、本サービスでは使用しない
Brevo	家族向けのDinner Questionsメール（登録後。電子メールアドレスのみ）	EU	家族向けニュースレターであり、本サービスでは使用しない
RevenueCat	アプリのサブスクリプションの状態（アカウント識別子および購入履歴のみ）	米国。標準契約条項	アプリのファミリーアカウント。学校のデータなし
Google Play / Apple App Store	アプリ内サブスクリプションの支払い。ストアが請求	EU／米国	ストアは独立した管理者としてサブスクリプションを販売する

サービス	業務内容	所在地	本契約の対象外である理由
Google / Apple（アプリのログイン）	アプリにおける保護者の任意のログイン（電子メールアドレスおよびログイン識別子）	EU／米国。EU・米国データプライバシー・フレームワーク、標準契約条項	アプリのファミリーアカウント。学校のデータなし
UptimeRobot	公開ページおよびステータスのエンドポイントが応答することを確認	EU／米国	個人データを処理しない

附属書IV — 子どものデータ

本附属書は、18歳未満の児童・生徒について附属書IおよびIIを補足する。

1. **デジタル同意年齢。** 子どもに直接提供される情報社会サービスについて管理者に適用される法が同意を求める場合（GDPR第8条）、管理者がこれを取得し記録する。その年齢は、スペインでは14歳（LOPDGDD第7条）、その他のEU加盟国では13〜16歳、英国では13歳である。米国の学校については附属書Vを参照。管理者が学校での利用を公共の利益のための任務など別の法的根拠に基づかせる場合、同意は不要であり、管理者が児童・生徒および親に情報を提供する。本サービスは年齢を確認しない。2つの年齢グループ（9〜12歳および13〜17歳）は、コンテンツおよび動画の版を選ぶためだけのものである。
2. **ウェブサイトにおける保護者同意の手続。** ウェブサイトの機能がデジタル同意年齢に満たない子どもについて親の同意を必要とする場合、本サービスは、電子メールで送られる1回限りのリンクにより親が確認するまで何も保存しない。保存されるのは、親の電子メールアドレスの鍵付きハッシュ、判断およびタイムスタンプのみである。未回答の依頼は30日後に、拒否は12か月後に削除される。同意を撤回すると、それに基づいて収集されたデータが削除される。
3. **ファミリープラン。** 親または保護者がファミリーサブスクリプションを契約し、処理者の顧客となる。ウェブサイトでは、支払い時に購入者が成年であることの確認を求める。アプリでは、ログインおよび購入は大人向けの確認（入力する計算問題）の後ろにある。いずれも本人確認や年齢確認ではない。子どもはウェブサイトでアカウントを作成しない。子どもは親の責任の下でファミリーコードを使用することができる。これに学校のデータは紐付かない。
4. **プロファイリングおよび広告の不実施。** 処理者は広告を表示せず、広告識別子や広告SDKを使用しない。管理者の教師が閲覧する進捗の記録を超えて児童・生徒のプロファイルを作成せず、法的効果またはそれと同様の重大な影響を及ぼす自動化された決定を行わず、児童・生徒のデータを広告のために販売または共有することは決してない。
5. **子ども向けページでの分析の不実施。** 子ども向けページ（アドベンチャーゲーム、ゲーム集、クイズ、ライブラリー、目標のページ、Wordle、ミッションおよび書籍。13言語すべて）は、分析、トラッカーおよび同意バナーを読み込まない。厳密に必要なブラウザ内の保存（言語、端末上の進捗、セッション）のみを使用する。
6. **効果測定調査。** 管理者がクラスを効果測定調査に登録する場合、児童・生徒は、管理者自身の授業の評価の一環として授業中に回答する。管理者は、事前に親に情報を提供して異議を述べる機会を与えるか、その法または規則が求める場合は書面による同意を得る。本サービスはいずれにも対応し、該当する席を除外する。児童・生徒はどの質問も飛ばすことができ、最初の画面でそのことを知らされる。教師はクラスの結果のみを、かつ少なくとも10人の児童・生徒が事前と事後の両方に回答した場合にのみ閲覧できる。学校のどの利用者も、児童・生徒個人の回答を閲覧することはない。子どもの保護に関わる打ち明けを含むおそれのある自由記述の回答は、管理者が指定した担当者に回され、その者が対応を決定する。処理者は、第2.3条に従い、集計され匿名化された結果のみを使用し、自由記述は決して使用しない。打ち明けの可能性があるものは、1授業日以内に指定された担当者に渡され、その担当者のみがこれを閲覧する。子どもの保護の担当者が指定されていない場合は、第4.4条に定める受領者がこれに代わる。
7. **コミュニケーション機能の不存在。** 本サービスには、チャット、メッセージおよび児童・生徒の公開プロフィールがない。クイズの公開ランキングは任意であり、生成されたリストからのニックネームのみを使用し、学校名を表示せず、記録を30日間保存し、各記録に報告用

のリンクがある。クラスのランキングは、そのクラスの教師および学校の管理担当者のみが閲覧でき、3回報告された公開の記録は確認されるまで非表示になる。

8. **管理者に伝える残存リスク。** クラスコードと児童・生徒のニックネームを知っている同級生は、別の端末でその児童・生徒の進捗を開くことができる。教師は、いつでも児童・生徒を閲覧し、名前を変更し、または削除することができ、クラスコードを更新することができる。管理者は、自らの評価およびクラスコードの配布方法においてこの点を考慮する。
9. **親および児童・生徒の権利。** 親および児童・生徒は、管理者に対して権利を行使する。管理者の教師は、児童・生徒のデータを直接閲覧し、エクスポートし、名前を変更し、リセットし、削除することができる。処理者は、受け取った請求を管理者に転送する（第8.2条）。
10. **子どもへの情報提供。** 処理者は、子ども向けに書かれた部分（第A部）と親および学校向けの部分（第B部）から成る子どものプライバシーに関する通知を https://eco-heroes.org/legal/children/ に掲載している。管理者は、児童・生徒および親への自らの情報提供にこれを使用することができる。

附属書V — 英国および米国の管理者

1. **英国。** 管理者が英国に設立されている場合、本契約におけるGDPRへの言及は、UK GDPRおよびData Protection Act 2018への言及と読み替えるものとし、管轄の監督機関はInformation Commissioner's Office（ICO）とする。管理者データは、欧州経済領域に関する英国の十分性規則に基づき英国から欧州経済領域に移転される。米国への再移転は、プロバイダーが認証を受けている場合はEU・米国データプライバシー・フレームワークの英国拡張に、それ以外の場合は標準契約条項に対するUK International Data Transfer Addendumに基づく。処理者は、ICOのAge Appropriate Design Codeを考慮して本サービスを設計しており、その遵守の概要はプライバシーポリシーの第11節に記載している。
2. **米国 — FERPA。** 管理者がFamily Educational Rights and Privacy Actの適用を受ける米国の学校または学区である場合、処理者は、34 CFR 99.31(a)(1)(i)(B)に基づく正当な教育上の利益を有する「school official」として行動する。処理者は、教育記録の使用および保守に関して管理者の直接の管理下にあり、これを本ライセンスの目的のためにのみ使用し、第6条に基づく再委託先に対する場合または法が求める場合を除き、他者に開示しない。
3. **米国 — COPPA。** 13歳未満の児童・生徒について、管理者は、連邦取引委員会のガイダンスが認めるとおり、附属書Iに記載するデータの収集に親に代わって同意することができる。これは、データが管理者の教育目的のためにのみ使用され、その他の商業目的には使用されないためである。管理者は親に情報を提供し続け、子どものデータの閲覧または削除を求める親の請求を転送する。処理者は第8条に従いこれに応じる。
4. **米国 — 削除および通知。** 本ライセンス終了時の削除には第10条が適用される。州の児童・生徒のプライバシーに関する法律が侵害の通知または削除についてより短い期限を定めている場合、処理者は、管理者がどの法律が適用されるかを示し次第、これを遵守する。
