Dies ist eine zur besseren Verständlichkeit bereitgestellte Übersetzung. Die englische Fassung ist der rechtsverbindliche Text und hat bei Abweichungen Vorrang. English (PDF)

Auftragsverarbeitungsvertrag

gemäß Artikel 28 der Verordnung (EU) 2016/679 (DSGVO) und Artikel 33 des spanischen Organgesetzes 3/2018 vom 5. Dezember über den Schutz personenbezogener Daten und die Gewährleistung digitaler Rechte (LOPDGDD) — zwischen dem Lizenznehmer (dem „Verantwortlichen“) und Eco Heroes International SL (dem „Auftragsverarbeiter“)

Parteien und Rollen

Verantwortlicher: _____ (Name der Schule, des Schulverbunds, der Bildungsbehörde, des Unternehmens oder des Hotels gemäß Lizenz), mit Sitz in _____, vertreten durch _____ (Name, Funktion).
Datenschutzkontakt des Verantwortlichen (Administratorkontakt oder, falls benannt, Datenschutzbeauftragter): _____.

Auftragsverarbeiter: Eco Heroes International SL, CIF B44915940, mit Sitz in 17003 Girona (Spanien), eingetragen im Registro Mercantil de Girona, vertreten durch Karim Zouhdi, Gründer. Datenschutzkontakt: info@eco-heroes.org, +34 690 814 215. Sicherheitsmeldungen: security@eco-heroes.org (siehe https://eco-heroes.org/.well-known/security.txt).

Rollen. Der Verantwortliche entscheidet, warum und wie die Daten des Verantwortlichen verarbeitet werden, und ist für sie verantwortlich. Der Auftragsverarbeiter verarbeitet die Daten des Verantwortlichen ausschließlich im Auftrag des Verantwortlichen, als Auftragsverarbeiter im Sinne von Artikel 4 Nummer 8 DSGVO.

Lehrkräftekonten. Jede Lehrkraft hat ein eigenes, persönliches Konto. Der Auftragsverarbeiter betreibt das Konto selbst (Anmeldung, Sicherheit, Zwei-Faktor-Anmeldung und die kostenlosen Lehrkräfte-Materialien) als Verantwortlicher nach seiner Datenschutzerklärung. Alles, was eine Lehrkraft im Dienst für den Verantwortlichen tut, sind Daten des Verantwortlichen: die Rolle und die Rechte des Kontos in der Organisation des Verantwortlichen, Klassen, Schülerinnen und Schüler, Fortschritt, Aufgaben, Live-Quiz, Klassenlisten-Importe, Starts aus der Lernplattform und Wirkungsstudien.

Nicht Gegenstand dieses Vertrags. Anhang I Abschnitt B nennt die Verarbeitungen, für die der Auftragsverarbeiter selbst verantwortlich ist. Für sie gilt die Datenschutzerklärung des Auftragsverarbeiters (https://eco-heroes.org/legal/privacy/), nicht dieser Vertrag. Die Eco Heroes Academy (learn.eco-heroes.org) und das VSME-Assessment (assessment.eco-heroes.org) sind eigenständige Dienste mit eigenen Bedingungen und Datenschutzhinweisen; dieser Vertrag erfasst sie nicht.

Dieser Vertrag ist Bestandteil der Lizenz. Bei Widersprüchen zwischen der Lizenz und diesem Vertrag in Bezug auf die Verarbeitung personenbezogener Daten hat dieser Vertrag Vorrang.

Begriffsbestimmungen

- **„Lizenz“** bezeichnet den Vertrag, auf dessen Grundlage der Verantwortliche den Dienst nutzt: das vom Verantwortlichen angenommene Angebot oder die Bestellung sowie die unter https://eco-heroes.org/legal/licence/ veröffentlichten Lizenzbedingungen für Schulen und Organisationen.
- **„Dienst“** bezeichnet die Eco-Heroes-Plattform und den Support gemäß Klausel 1.1.
- **„Daten des Verantwortlichen“** bezeichnet die personenbezogenen Daten, die der Auftragsverarbeiter im Rahmen dieses Vertrags im Auftrag des Verantwortlichen verarbeitet, wie in Anhang I Abschnitt A beschrieben.
- **„Nutzer“** bezeichnet die Schülerinnen und Schüler, Lehrkräfte, Schuladministratoren, Beschäftigten, Mitarbeitenden, Gäste und sonstigen Personen, die der Verantwortliche zur Nutzung des Dienstes berechtigt.
- **„Unterauftragsverarbeiter“** bezeichnet einen weiteren Auftragsverarbeiter, den der Auftragsverarbeiter zur Verarbeitung von Daten des Verantwortlichen einsetzt.
- **„Werktag“** bezeichnet Montag bis Freitag mit Ausnahme der Feiertage in Girona (Spanien).
- Begriffe, die in Artikel 4 DSGVO bestimmt sind, wie „personenbezogene Daten“, „Verarbeitung“ und „Verletzung des Schutzes personenbezogener Daten“, haben in diesem Vertrag dieselbe Bedeutung.

1. Gegenstand und Dauer

1.1 Der Auftragsverarbeiter erbringt den Dienst für den Verantwortlichen im Rahmen der Lizenz. Der Dienst umfasst: das Abenteuerspiel, das Quiz, die Wortspiele und die Live-Klassenquiz; die Bilderbücher und die Story Library, die Missionsvideos, die Handbücher und die Unterrichtsblätter; persönliche Lehrkräftekonten, Klassenverwaltung und Aufgaben; den optionalen Import von Klassenlisten (CSV, OneRoster-CSV, Google Classroom); die optionale Anmeldung der Lehrkräfte mit Google oder Microsoft; die optionale Anbindung an die Lernplattform des Verantwortlichen über LTI 1.1 oder LTI 1.3; das Klassen-Dashboard der mobilen Eco-Heroes-App, sofern der Verantwortliche es nutzt; optionale Wirkungsstudien; bei Unternehmens- und Hotellizenzen Koordinatorenkonten, Gruppen mit Beitrittscodes für die Kinder von Beschäftigten oder Gästen und Fortschrittsberichte je Gruppe (CSV), einen zusammengefassten Organisationsbericht, Urkunden mit dem Namen der Organisation und die optionale Anmeldung der Mitarbeitenden über den eigenen Identitätsanbieter des Verantwortlichen; sowie Support.

1.2 Der Auftragsverarbeiter verarbeitet Daten des Verantwortlichen während der Laufzeit der Lizenz und so lange, bis alle Daten des Verantwortlichen nach Klausel 10 gelöscht oder zurückgegeben sind.

2. Art und Zweck der Verarbeitung; Kategorien

2.1 **Anhang I** beschreibt Art und Zweck der Verarbeitung, die Kategorien betroffener Personen und die Kategorien personenbezogener Daten.

2.2 Der Auftragsverarbeiter verarbeitet Daten des Verantwortlichen ausschließlich, um den Dienst für den Verantwortlichen zu erbringen. Er verwendet sie nicht für Werbung, nicht zur Erstellung von Schülerprofilen über den Lernfortschritt hinaus, den der Dienst den Lehrkräften des Verantwortlichen

zeigt, nicht zum Verkauf oder zur Vermietung von Daten und nicht zur Entwicklung eines anderen Produkts als des Dienstes.

2.3 **Anonymisierte Statistiken.** Wenn der Verantwortliche Klassen für eine Wirkungsstudie anmeldet, weist er den Auftragsverarbeiter an, aus den Antworten zusammengefasste Statistiken zu erstellen, die der Auftragsverarbeiter in eigenen Berichten und Veröffentlichungen verwenden darf. Der Auftragsverarbeiter fasst nur Antworten aus Gruppen von mindestens 10 Schülerinnen und Schülern zusammen, bezieht niemals Freitextantworten ein und prüft, dass keine Schülerin, kein Schüler, keine Klasse und keine Schule identifiziert werden kann. Die so erstellten Statistiken sind keine personenbezogenen Daten mehr. Der Verantwortliche kann diese Weisung jederzeit durch schriftliche Mitteilung widerrufen; danach erhobene Antworten werden nur für die eigenen Ergebnisse des Verantwortlichen verwendet.

3. Weisungen

3.1 Der Auftragsverarbeiter verarbeitet Daten des Verantwortlichen nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder eines Mitgliedstaats, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die dokumentierten Weisungen des Verantwortlichen sind dieser Vertrag, die Lizenz und die Einstellungen, die der Verantwortliche und seine Nutzer im Dienst wählen (zum Beispiel Klassen anlegen, Klassenlisten importieren, Single Sign-on oder eine Lernplattform-Anbindung aktivieren, eine Klasse für eine Wirkungsstudie anmelden, Schülerinnen und Schüler oder Klassen löschen). Weitere Weisungen erteilt der Administratorkontakt des Verantwortlichen schriftlich; eine E-Mail an info@eco-heroes.org genügt.

3.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn eine Weisung seiner Auffassung nach gegen die DSGVO, die LOPDGDD oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter kann die Ausführung dieser Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

4. Pflichten des Verantwortlichen

4.1 Der Verantwortliche ist verantwortlich für die Rechtmäßigkeit der Verarbeitung, einschließlich der Rechtsgrundlage für die Verarbeitung der Schülerdaten; für die Bereitstellung der nach Artikel 13 und 14 DSGVO erforderlichen Informationen an die betroffenen Personen (Schülerinnen und Schüler sowie gegebenenfalls deren Eltern oder Erziehungsberechtigte, Lehrkräfte, Administratoren, Beschäftigte und Gäste); für die Einholung jeder Einwilligung, die das für den Verantwortlichen geltende Recht für Schülerinnen und Schüler unter dem Alter der digitalen Einwilligung verlangt (Artikel 8 DSGVO; Artikel 7 LOPDGDD: 14 Jahre in Spanien); und für die Richtigkeit der Daten, die er und seine Nutzer eingeben.

4.2 Der Verantwortliche weist seine Nutzer an, keine besonderen Kategorien personenbezogener Daten (Artikel 9 DSGVO), keine Nachnamen, E-Mail-Adressen oder anderen direkten Kennungen von Schülerinnen und Schülern in Freitextfelder einzugeben, etwa in Spitznamen, Klassennamen, Aufgabennotizen, Spitznamen im Live-Quiz und Umfrageantworten.

4.3 Wenn der Verantwortliche seine eigene Lernplattform (LTI) oder seinen Identitätsanbieter (Single Sign-on) anbindet, ist er für dieses System und dessen Konfiguration verantwortlich, damit es nur die

in Anhang I beschriebenen Daten weitergibt (für Schülerinnen und Schüler über LTI nur den Namen, niemals die E-Mail-Adresse).

4.4 Der Verantwortliche benennt einen Administratorkontakt und, bevor er eine Wirkungsstudie durchführt, eine Ansprechperson für Kinderschutz und hält beide Kontakte im Dienst oder per E-Mail an den Auftragsverarbeiter aktuell. Solange keine Ansprechperson für Kinderschutz benannt ist oder das Konto der benannten Person geschlossen ist, leitet der Dienst Kinderschutz-Hinweise an die Schuladministratoren des Verantwortlichen weiter. Bei Klassen, die im Dienst keiner Schule zugeordnet sind (zum Beispiel Klassen, die nur über einen LTI-Start genutzt werden), gehen die Hinweise an die für Kinderschutz verantwortliche Person des Auftragsverarbeiters, die sie unverzüglich an den Administratorkontakt des Verantwortlichen weitergibt.

5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter

a. verarbeitet Daten des Verantwortlichen ausschließlich nach Klausel 3;

b. gewährleistet, dass sich alle Personen, die zur Verarbeitung von Daten des Verantwortlichen befugt sind, vertraglich oder gesetzlich zur Vertraulichkeit verpflichtet haben, und dass der Zugang zu Produktivsystemen auf namentlich benannte Personen beschränkt ist, die ihn benötigen;

c. trifft die technischen und organisatorischen Maßnahmen nach **Anhang II** und gewährleistet ein dem Risiko angemessenes Schutzniveau nach Artikel 32 DSGVO, unter Berücksichtigung der Tatsache, dass zu den betroffenen Personen Kinder gehören;

d. nimmt die Dienste eines weiteren Auftragsverarbeiters nur unter den Bedingungen der Klausel 6 in Anspruch;

e. unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (Artikel 12 bis 23 DSGVO), wie in Klausel 8 geregelt;

f. unterstützt den Verantwortlichen bei der Einhaltung der Artikel 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen; die Zusammenfassung der aktuellen Datenschutz-Folgenabschätzung des Auftragsverarbeiters ist im Trust Centre veröffentlicht, und die vollständige Abschätzung wird dem Verantwortlichen auf Anfrage zur Verfügung gestellt;

g. löscht nach Wahl des Verantwortlichen nach Abschluss des Dienstes alle Daten des Verantwortlichen oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaats eine Verpflichtung zur Speicherung besteht (Klausel 10);

h. stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung von Artikel 28 DSGVO zur Verfügung und ermöglicht und unterstützt Überprüfungen, einschließlich Inspektionen, durch den Verantwortlichen oder einen von ihm beauftragten Prüfer (Klausel 11);

i. führt ein Verzeichnis aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten (Artikel 30 Absatz 2 DSGVO);

j. übermittelt Daten des Verantwortlichen nur unter den Bedingungen der Klausel 7 in ein Drittland.

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt eine allgemeine schriftliche Genehmigung für die in **Anhang III Teil A** aufgeführten Unterauftragsverarbeiter.

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens **30 Tage** im Voraus, per E-Mail an den Administratorkontakt des Verantwortlichen und durch Aktualisierung von https://eco-heroes.org/trust/. Der Verantwortliche kann aus berechtigten datenschutzrechtlichen Gründen Einspruch erheben. Lässt sich der Einspruch nicht innerhalb der Mitteilungsfrist ausräumen, kann der Verantwortliche den betroffenen Teil der Lizenz ohne Vertragsstrafe kündigen; es gilt Klausel 10.

6.3 Der Auftragsverarbeiter setzt jeden Unterauftragsverarbeiter auf Grundlage der Standard-Datenverarbeitungsbedingungen dieses Anbieters ein. Diese Bedingungen erlegen dem Unterauftragsverarbeiter Datenschutzpflichten auf, die hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bieten, wie Artikel 28 Absatz 4 DSGVO es verlangt. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass jeder Unterauftragsverarbeiter diese Pflichten erfüllt.

6.4 **Anhang III Teil B** nennt Dienste Dritter, die der Auftragsverarbeiter nutzt, die aber **keine** Daten des Verantwortlichen verarbeiten. Sie verarbeiten keine personenbezogenen Daten oder nur solche, für die der Auftragsverarbeiter selbst verantwortlich ist. Sie werden der Transparenz halber genannt und sind keine Unterauftragsverarbeiter im Sinne dieses Vertrags.

6.5 Die eigenen Systeme des Verantwortlichen, etwa seine Lernplattform oder seine Google- oder Microsoft-Umgebung, werden vom Verantwortlichen ausgewählt und kontrolliert. Sie sind keine Unterauftragsverarbeiter des Auftragsverarbeiters.

7. Internationale Übermittlungen

7.1 Die Daten des Verantwortlichen werden in der Europäischen Union gehostet und gespeichert: die Anwendungsserver in Frankreich (Internet Girona, auf Infrastruktur von OVHcloud); die Datenbank, die verschlüsselten Sicherungen und ein Ausweichserver in Deutschland und Finnland (Hetzner Online GmbH). Das Content-Delivery-Netzwerk (Cloudflare) liefert zwischengespeicherte öffentliche Seiten aus seinem weltweiten Netz aus. Antworten mit personenbezogenen Daten sind als privat und nicht speicherbar (no-store) gekennzeichnet, und das Netz speichert sie nicht zwischen.

7.2 Der Auftragsverarbeiter übermittelt keine Daten des Verantwortlichen außerhalb des Europäischen Wirtschaftsraums und gestattet dies keinem Unterauftragsverarbeiter, es sei denn, (i) für das Ziel besteht ein Angemessenheitsbeschluss der Europäischen Kommission, einschließlich der Schweiz und, für Organisationen, deren Zertifizierung der Auftragsverarbeiter in der offiziellen Liste geprüft hat, des EU-US-Datenschutzrahmens; oder (ii) auf Grundlage der mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission erlassenen Standardvertragsklauseln (Modul 3, Auftragsverarbeiter an Auftragsverarbeiter, oder gegebenenfalls Modul 2), ergänzt um zusätzliche Maßnahmen, wenn eine Übermittlungsbewertung zeigt, dass sie erforderlich sind. Anhang III nennt die für jeden Unterauftragsverarbeiter geltende Garantie. Der Auftragsverarbeiter hält für jeden Unterauftragsverarbeiter außerhalb des EWR eine schriftliche Übermittlungsbewertung vor und stellt sie dem Verantwortlichen auf Anfrage zur Verfügung.

7.3 Cloudflare, Inc. beendet die verschlüsselte Verbindung am Rand seines Netzes und verarbeitet dort daher Anfragedaten (IP-Adresse, aufgerufene Adresse, Header). Der Auftragsverarbeiter stützt sich auf die Standard-Datenverarbeitungsbedingungen von Cloudflare mit den Standardvertragsklauseln und, sofern Cloudflare in der offiziellen Liste des Datenschutzrahmens geführt wird, auf den EU-US-Datenschutzrahmen.

7.4 Proton AG hostet die E-Mail des Auftragsverarbeiters in der Schweiz. Für die Schweiz besteht ein Angemessenheitsbeschluss der Europäischen Kommission.

8. Unterstützung bei der Wahrnehmung von Betroffenenrechten

8.1 Lehrkräfte können die Daten einer Schülerin oder eines Schülers direkt im Dienst einsehen, exportieren (CSV), umbenennen, zurücksetzen und löschen sowie ganze Klassen löschen. Jede Lehrkraft sieht nur ihre eigenen Klassen; Schuladministratoren sehen alle Klassen ihrer Schule und können einer Lehrkraft den Zugang sofort entziehen. Der Verantwortliche nutzt diese Funktionen, um Anträge zu beantworten, wann immer dies möglich ist.

8.2 Kann ein Antrag nicht über den Dienst erfüllt werden, unterstützt der Auftragsverarbeiter den Verantwortlichen innerhalb von **10 Werktagen** nach einer schriftlichen Anfrage. Erhält der Auftragsverarbeiter einen Antrag zu Daten des Verantwortlichen direkt von einer betroffenen Person (einschließlich eines Elternteils oder Erziehungsberechtigten), beantwortet er ihn nicht in der Sache. Er verweist die betroffene Person unverzüglich an den Verantwortlichen und informiert den Verantwortlichen, sofern dieser nichts anderes angewiesen hat.

9. Verletzung des Schutzes personenbezogener Daten

9.1 Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich und spätestens **48 Stunden**, nachdem sie ihm bekannt geworden ist. Die erste Meldung enthält die nach Artikel 33 Absatz 3 DSGVO erforderlichen Informationen, soweit sie zu diesem Zeitpunkt bekannt sind: die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Der Auftragsverarbeiter ergänzt diese Informationen schrittweise, sobald sie verfügbar werden.

9.2 Der Auftragsverarbeiter arbeitet mit dem Verantwortlichen zusammen, um die Verletzung zu untersuchen, einzudämmen und zu dokumentieren, und unterstützt ihn bei jeder Meldung an die Aufsichtsbehörde (in Spanien die Agencia Española de Protección de Datos) und bei jeder Benachrichtigung der betroffenen Personen. Der Auftragsverarbeiter dokumentiert jede Verletzung des Schutzes personenbezogener Daten einschließlich der Fakten, ihrer Auswirkungen und der ergriffenen Maßnahmen.

9.3 Der Auftragsverarbeiter sendet Meldungen per E-Mail an den Administratorkontakt des Verantwortlichen. Jede Person kann eine Sicherheitslücke an security@eco-heroes.org melden. Meldungen werden innerhalb von 5 Werktagen bestätigt, und kritische Probleme werden vor allen anderen Arbeiten behoben.

10. Aufbewahrung, Löschung und Rückgabe

10.1 **Während der Lizenz.** Die Daten des Verantwortlichen werden nach dem Plan in Anhang I Abschnitt C aufbewahrt, der die im Code des Dienstes umgesetzten Aufbewahrungsregeln wiedergibt. Eine Lehrkraft kann eine Schülerin, einen Schüler oder eine Klasse jederzeit löschen, mit sofortiger Wirkung in der aktiven Datenbank und im Ausweich-Replikat.

10.2 **Export.** Während der Lizenz und bis zur Löschung nach Klausel 10.3 kann der Verantwortliche Klassen- und Fortschrittsdaten im Dienst als CSV exportieren oder vom Auftragsverarbeiter einen Export in einem strukturierten, gängigen und maschinenlesbaren Format verlangen.

10.3 **Ende der Lizenz.** Endet die Lizenz und wird sie nicht verlängert, löscht der Auftragsverarbeiter die Daten des Verantwortlichen **90 Tage** nach dem Enddatum. Verlangt der Verantwortliche dies schriftlich, löscht der Auftragsverarbeiter die Daten des Verantwortlichen innerhalb von **30 Tagen** nach dem Verlangen, unabhängig davon, ob die Lizenz geendet hat. Der Auftragsverarbeiter bestätigt

die Löschung auf Anfrage schriftlich. Vor der Löschung schreibt der Auftragsverarbeiter den Schuladministratoren des Verantwortlichen 30 Tage und 7 Tage vor dem Löschdatum eine E-Mail mit diesem Datum und dem Hinweis, wie die Lizenz verlängert oder die Daten exportiert werden können; die Löschung erfolgt frühestens 30 Tage nach der ersten und 7 Tage nach der zweiten Nachricht.

10.4 **Lehrkräftekonten.** Wenn die letzte mit einem Lehrkräftekonto verbundene Lizenz endet, wird das Konto als kostenloses Lehrkräftekonto fortgeführt. Es wird 12 Monate nach dem Ende dieser Lizenz gelöscht, sofern die Lehrkraft nicht zwischenzeitlich einer neuen Lizenz zugeordnet wird; ein kostenloses Konto wird nach 12 Monaten ohne Anmeldung gelöscht. Der Auftragsverarbeiter schreibt der Lehrkraft 30 Tage vor der Löschung eine E-Mail. Die Fortführung eines Lehrkräftekontos bewahrt keine Daten des Verantwortlichen auf: Diese werden nach Klausel 10.3 gelöscht.

10.5 **Sicherungen und Replikat.** Gelöschte Daten verschwinden im normalen Zyklus aus den Sicherungen. Die verschlüsselten Sicherungen werden rollierend aufbewahrt, sodass gelöschte Daten innerhalb von **14 Tagen** aus allen Sicherungen verschwinden. Das schreibgeschützte Replikat auf dem Ausweichserver vollzieht jede Löschung laufend nach. Sicherungen werden nur wiederhergestellt, um einen Verlust des Produktivsystems zu beheben; stellt eine Wiederherstellung gelöschte Daten wieder her, wird die Löschung erneut angewendet.

10.6 **Gesetzliche Aufbewahrung.** Der Auftragsverarbeiter bewahrt personenbezogene Daten nach dem Ende der Lizenz nur auf, soweit und solange das Unionsrecht oder das Recht eines Mitgliedstaats dies verlangt, zum Beispiel Rechnungen und Buchhaltungsunterlagen 6 Jahre lang nach Artikel 30 des spanischen Handelsgesetzbuchs (Código de Comercio). Diese Unterlagen nennen die Kontaktpersonen des Verantwortlichen und enthalten keine Schülerdaten. Der Auftragsverarbeiter schützt sie nach Anhang II und verwendet sie zu keinem anderen Zweck.

11. Prüfung und Information

11.1 Auf Anfrage und höchstens einmal pro Vertragsjahr (oder zusätzlich nach einer Verletzung des Schutzes personenbezogener Daten oder bei einem dokumentierten, begründeten Verdacht auf Nichteinhaltung) stellt der Auftragsverarbeiter dem Verantwortlichen die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind. Dazu gehören die aktuelle Sicherheitszusammenfassung (https://eco-heroes.org/trust/#security), die aktuelle Liste der Unterauftragsverarbeiter, das Verzeichnis der im Auftrag des Verantwortlichen durchgeführten Verarbeitungen, die Übermittlungsbewertungen, die Datenschutz-Folgenabschätzung, die letzten Ergebnisse der Wiederherstellungstests und Umschaltübungen sowie die Ergebnisse etwaiger Sicherheitsprüfungen.

11.2 Reichen diese Informationen nicht aus, kann der Verantwortliche oder ein von ihm beauftragter, zur Vertraulichkeit verpflichteter unabhängiger Prüfer die betreffenden Verarbeitungen des Auftragsverarbeiters mit einer Ankündigungsfrist von mindestens **30 Tagen** prüfen, während der Geschäftszeiten und ohne unangemessene Störung des Betriebs des Auftragsverarbeiters oder anderer Kunden. Jede Partei trägt ihre eigenen Kosten. Der Auftragsverarbeiter kann vom Prüfer die Unterzeichnung einer angemessenen Vertraulichkeitsvereinbarung verlangen und den Zugang zu Systemen, die mit anderen Kunden geteilt werden, auf das zur Prüfung der Einhaltung Erforderliche beschränken.

12. Haftung

12.1 Jede Partei haftet gegenüber den betroffenen Personen nach Artikel 82 DSGVO. Im Verhältnis der Parteien zueinander richtet sich die Haftung nach der Haftungsklausel der Lizenz. Keine Bestimmung dieses Vertrags oder der Lizenz beschränkt die Haftung einer Partei, soweit das Gesetz eine Beschränkung nicht zulässt, einschließlich der Haftung für Vorsatz.

12.2 Muss der Auftragsverarbeiter wegen der Weisungen des Verantwortlichen oder weil dieser seine Pflichten nach Klausel 4 nicht erfüllt hat, ein Bußgeld oder Schadensersatz zahlen, stellt der Verantwortliche den Auftragsverarbeiter im Umfang dieser Ursache frei, und umgekehrt.

13. Laufzeit, anwendbares Recht und Gerichtsstand

13.1 Dieser Vertrag tritt mit dem Beginn der Lizenz in Kraft und endet, wenn alle Daten des Verantwortlichen nach Klausel 10 gelöscht oder zurückgegeben sind. Die Klauseln 5(b), 10, 11 und 12 gelten so lange fort, wie es erforderlich ist.

13.2 Dieser Vertrag unterliegt spanischem Recht und dem Recht der Europäischen Union, einschließlich der DSGVO und der LOPDGDD. Zuständig sind die Gerichte von Girona (Spanien), unbeschadet zwingender Vorschriften, die für den Verantwortlichen als öffentliche Stelle oder nach dem Vergaberecht gelten, und unbeschadet der Rechte der betroffenen Personen nach Artikel 79 DSGVO. Anhang V ergänzt die Regeln für Verantwortliche im Vereinigten Königreich und in den Vereinigten Staaten.

13.3 Änderungen dieses Vertrags bedürfen der Schriftform; eine E-Mail genügt. Der Auftragsverarbeiter veröffentlicht die aktuelle Vorlage unter https://eco-heroes.org/trust/. Eine neue Fassung der Vorlage ändert einen unterzeichneten Vertrag nicht ohne Zustimmung des Verantwortlichen. Der Schuladministrator des Verantwortlichen kann diesen Vertrag online annehmen; der Auftragsverarbeiter speichert, wer ihn angenommen hat, wann, welche Fassung und einen schlüsselbasierten Hash der verwendeten IP-Adresse.

Unterschriften

Für den Verantwortlichen

Name, Funktion
Datum, Unterschrift

Für den Auftragsverarbeiter — Eco Heroes International SL

Karim Zouhdi, Gründer
Datum, Unterschrift

Anhang I — Beschreibung der Verarbeitung

A. Verarbeitung im Auftrag des Verantwortlichen (Gegenstand dieses Vertrags)

Anhang I.A — Verarbeitung im Auftrag des Verantwortlichen

Punkt	Beschreibung
Gegenstand	Bereitstellung des Dienstes für die Nutzer des Verantwortlichen im Rahmen der Lizenz.
Art	Hosting, Speicherung, Anzeige und Löschung von Daten; Fortschrittsverfolgung; Live-Klassenquiz; Aufgaben; Zertifikate; Klassenverwaltung; optionaler Import vom Verantwortlichen bereitgestellter Klassenlisten (CSV einfügen oder hochladen, OneRoster-CSV 1.1/1.2, Google Classroom); optionale Starts über LTI 1.1 / LTI 1.3 aus der Lernplattform des Verantwortlichen, mit Names and Role Provisioning (Klassenlisten-Import) und Assignment and Grade Services (Rückgabe von Punktzahlen); optionale, vom Verantwortlichen gewählte Anmeldung der Lehrkräfte mit Google oder Microsoft; Klassen-Dashboard der mobilen Eco-Heroes-App, wenn der Verantwortliche einen Klassencode ausgibt; optionale Fragebögen für Wirkungsstudien in vom Verantwortlichen angemeldeten Klassen; Koordinatorenkonten, Gruppen-Beitrittscodes und Fortschrittsberichte je Gruppe (CSV) für Unternehmens- und Hotellizenzen; Support. Bei Unternehmens- und Hotellizenzen außerdem: zusammengefasste Aktivitätsberichte für die Organisation (Organisationsbericht und Summen, wobei jede Zahl, die auf weniger als 5 Familien beruht, ausgeblendet wird) und eine optionale Team-Rangliste; Name und Logo der Organisation auf den Urkunden der Kinder; optionale Anmeldung der Mitarbeitenden über den eigenen Identitätsanbieter des Verantwortlichen (OpenID Connect).
Zweck	Bildung für nachhaltige Entwicklung auf Grundlage der Ziele für nachhaltige Entwicklung der Vereinten Nationen, mit der in der Lizenz vorgesehenen Fortschrittsverfolgung, Berichterstattung und Bewertung. Bei Wirkungsstudien: die Bewertung des eigenen Unterrichts durch den Verantwortlichen (Klassenergebnisse für seine Lehrkräfte) und zusammengefasste, anonymisierte Statistiken nach Klausel 2.3. Kein anderer Zweck.
Kategorien betroffener Personen	Schülerinnen und Schüler (das Spiel ist für 9- bis 17-Jährige in zwei Altersgruppen, 9–12 und 13–17, konzipiert; die druckbaren Unterrichtsblätter decken die Stufen 6–10, 11–13 und 14–17 Jahre ab, und der Verantwortliche kann den Dienst nach eigenem Ermessen mit jüngeren Schülerinnen und Schülern nutzen); Lehrkräfte; Schuladministratoren; Eltern und Erziehungsberechtigte, nur wenn das Einwilligungsverfahren genutzt wird; bei Unternehmens- und Hotellizenzen die Kinder von Beschäftigten oder Gästen sowie die Koordinatorinnen und Koordinatoren der Organisation.

Punkt	Beschreibung
Personenbezogene Daten — Schülerinnen und Schüler (Website, in einer Klasse)	Vorname oder Spitzname, den die Schülerin bzw. der Schüler oder die Lehrkraft eingibt (2 bis 24 Zeichen; aus Klassenlisten-Importen Vorname und Initiale, nur zur Unterscheidung zweier Schülerinnen oder Schüler mit gleichem Vornamen auf höchstens die ersten 3 Buchstaben des Nachnamens erweitert — niemals der vollständige Name); im Spiel gewählte Altersgruppe (9–12 oder 13–17); Avatar aus einer festen Auswahl; Sprache; Fortschritt (Punkte, abgeschlossene Ziele und Missionen, Quiz-Sterne, Zahl der beantworteten und richtig beantworteten Fragen je Thema); erledigte Aufgaben; Datum des Beitritts und der letzten Aktivität; ein zufälliges Klassentoken, das auf dem Gerät der Schülerin bzw. des Schülers gespeichert wird, damit der Fortschritt gesichert werden kann. In einem Live-Klassenquiz: der eingegebene Spitzname, Antworten, Antwortzeiten und Punktzahl. Nicht erhoben werden: E-Mail-Adresse, Nachname, Foto, Geburtsdatum, Postanschrift, Standort, Geräte- oder Werbekennungen.
Personenbezogene Daten — Schülerinnen und Schüler (LTI-Starts)	Ein schlüsselbasierter Hash der Nutzerkennung der Plattform (um eine Schülerin oder einen Schüler einem Platz zuzuordnen); die Nutzerkennung der Plattform im Startdatensatz für 90 Tage, nur wenn die Plattform den Bewertungsdienst gewährt hat (für die Rückgabe von Punktzahlen erforderlich); Vorname und Initiale des Nachnamens als Spitzname; Kurskennung und Kurstitel; Rollen; Gebietsschema; zuletzt übermittelte Punktzahl. Weder E-Mail-Adresse noch vollständiger Name werden gespeichert; der Verantwortliche konfiguriert seine Plattform so, dass sie nur den Namen weitergibt.
Personenbezogene Daten — Schülerinnen und Schüler (mobile App, Klassen-Dashboard)	Aktivität (gespieltes Tagesspiel, Datum, Sprache, Punkte, Abschluss, Dauer; erreichte Ziele, Abzeichen) und ein Einweg-Hash einer zufälligen Installationskennung, die die App erzeugt. Schülerinnen und Schüler erscheinen der Lehrkraft unter einem generierten Alias. Das Dashboard zeigt für eine Klasse mit weniger als fünf aktiven Schülerinnen und Schülern nichts an.
Personenbezogene Daten — Schülerinnen und Schüler (Wirkungsstudie, wenn der Verantwortliche eine Klasse anmeldet)	Antworten auf den Studienfragebogen (Auswahlantworten, Bewertungen und optionale kurze Freitextantworten), Fragebogenversion, Sprache, Altersgruppe, Start- und Absendezeit sowie Qualitätsmerkmale. E-Mail-Adressen und Telefonnummern werden beim Eingang aus dem Freitext entfernt. Antworten, die einen kinderschutzrelevanten Hinweis enthalten können, werden der vom Verantwortlichen benannten Ansprechperson gemeldet. Die Antworten werden zwischen den Befragungsrunden über einen schlüsselbasierten Einweg-Hash des Platzes der Schülerin bzw. des Schülers in der Klasse verknüpft; weder Name noch E-Mail-Adresse noch Geburtsdatum werden erhoben. Für jeden Platz der vom Verantwortlichen erfasste Widerspruch oder die schriftliche Einwilligung. Ist keine Ansprechperson für Kinderschutz benannt, treten die in Klausel 4.4 genannten Empfänger an ihre Stelle.
Personenbezogene Daten — Lehrkräfte und Schuladministratoren	Name, dienstliche E-Mail-Adresse, Schule, Rolle (Lehrkraft oder Schuladministrator), Sprache; Passwort (bcrypt-Hash) oder Single-Sign-on-Kennung; Zwei-Faktor-Geheimnis und gehashte Wiederherstellungscodes bei Aktivierung (für Schuladministratoren verpflichtend); Status der E-Mail-Bestätigung; Anmeldezeiten und -anzahl; Sitzungen; angelegte Klassen; Vorschauen von Klassenlisten-Importen (nur Namen, 30 Minuten in der Sitzung gespeichert); Einträge im Audit-Protokoll administrativer Handlungen (mit einem schlüsselbasierten Hash der IP-Adresse und dem Land der Verbindung als 2-Buchstaben-Code aus dem Content-Delivery-Netzwerk); Support-Korrespondenz.

Punkt	Beschreibung
Personenbezogene Daten — Lehrkräfte (Wirkungsstudie)	Antworten auf den Lehrkräftefragebogen und, für Schülerinnen und Schüler von 6 bis 8 Jahren, der Beobachtungsbogen der Klasse, verknüpft über einen schlüsselbasierten Einweg-Hash des Kontos oder Codes der Lehrkraft; die Anmeldung der Klasse, ihr Einwilligungsmodus und ihre Zuordnung zu einer Studiengruppe.
Personenbezogene Daten — Eltern und Erziehungsberechtigte	Nur wenn das Einwilligungsverfahren der Website für eine Schülerin oder einen Schüler unter dem Alter der digitalen Einwilligung genutzt wird: ein schlüsselbasierter Einweg-Hash der E-Mail-Adresse des Elternteils (die Adresse selbst wird nur einmal zum Versand des Bestätigungslinks verwendet und nicht gespeichert), die Entscheidung und ihre Zeitstempel.
Personenbezogene Daten — Kinder und Koordinatoren (Unternehmens- und Hotellizenzen)	Kinder von Beschäftigten oder Gästen des Verantwortlichen: Sie treten einer Gruppe mit dem Beitrittscode des Verantwortlichen und einem Heldennamen (Spitznamen) auf dem eigenen oder einem Familiengerät bei, ohne Konto und ohne E-Mail-Adresse. Der Dienst speichert dieselben Daten wie für Schülerinnen und Schüler in einer Klasse: Heldenname, Altersgruppe, Avatar, Sprache, Fortschritt und Quiz-Ergebnisse. Koordinatorinnen und Koordinatoren: Name, dienstliche E-Mail-Adresse, Passwort-Hash oder Anmeldekennung, Einstellungen zur Zwei-Faktor-Anmeldung und die Gruppen, die sie anlegen. Die Koordination sieht erreichte Ziele und Quiz-Ergebnisse je Gruppe und kann sie als CSV exportieren. Für den Organisationsbericht erfasst der Dienst bei jedem Heldenprofil dieser Gruppen außerdem die Tage mit Aktivität und den Tag, an dem jedes Ziel und jede Mission zum ersten Mal abgeschlossen wurde (tagesgenau; Schulklassen werden so nicht erfasst). Berichte enthalten nur zusammengefasste Werte: keinen Namen, Spitznamen, keine Kennung und keine Zeile pro Kind; jede Zahl, die auf 1 bis 4 Familien beruht, wird ausgeblendet (k = 5), und eine zweite Zahl wird ausgeblendet, wenn sich die erste sonst errechnen ließe. Die Teambezeichnungen wählt der Administrator des Verantwortlichen; sie dürfen keine Personen benennen. Schaltet der Verantwortliche die Firmen-Anmeldung ein, stammen Namen und E-Mail-Adressen der Mitarbeitenden vom eigenen Identitätsanbieter des Verantwortlichen (Scopes openid, email und profile); dieser Identitätsanbieter ist ein eigenes System und ein eigener Auftragsverarbeiter des Verantwortlichen, kein Unterauftragsverarbeiter, und seine Subjektkennung wird nur als schlüsselbasierter Hash gespeichert. Co-Branding: der Anzeigename und das Logo der Organisation, die der Verantwortliche bereitstellt. Die öffentliche Abzeichenseite, die ein Elternteil oder eine sorgeberechtigte Person auf LinkedIn teilen kann, enthält keine personenbezogenen Daten (eine Zahl von Zielen, den Namen der Organisation, sofern der Verantwortliche zugestimmt hat, und eine Sprache, alles aus ihrem Link); das Teilen löst der Erwachsene aus, und der Auftragsverarbeiter sendet nichts an LinkedIn.
Besondere Kategorien (Artikel 9 DSGVO)	Keine werden abgefragt oder benötigt. Siehe Klausel 4.2.
Häufigkeit	Fortlaufend während der Laufzeit der Lizenz.

B. Verarbeitungen, für die Eco Heroes eigenständig verantwortlich ist (nicht Gegenstand dieses Vertrags)

Hier genannt, damit der Verantwortliche sieht, wo dieser Vertrag endet. Für sie gelten die Datenschutzerklärung (v4.3) und der Datenschutzhinweis für Kinder (v2.2) des Auftragsverarbeiters, nicht

dieser Vertrag:

- **Lehrkräftekonten als solche:** Anmeldung, Sicherheit, Zwei-Faktor-Anmeldung und die kostenlosen Lehrkräfte-Materialien. Der Auftragsverarbeiter ist für das Konto selbst verantwortlich und löscht es nach Klausel 10.4; die Aktivität des Kontos für den Verantwortlichen sind Daten des Verantwortlichen.
- **Kostenlose Lehrkräftekonten:** Lehrkräfte ohne Zuordnung zu einer Lizenz, die die kostenlosen Lehrkräfte-Materialien mit einer bestätigten E-Mail-Adresse nutzen.
- **Familienabonnements** auf der Website, abgeschlossen von einem Elternteil oder Erziehungsberechtigten: die E-Mail-Adresse (teilweise maskiert gespeichert), Stripe-Zahlungs- und Abonnementreferenzen und ein persönlicher Zugangscode (als schlüsselbasierter Hash gespeichert). Kartendaten erreichen den Auftragsverarbeiter nie. Ein in der Schule verwendeter Familiencode trägt keine Daten der Schule.
- **App-Konten** (Anmeldung der Eltern mit Google oder Apple; Abonnements über Google Play oder Apple; Abonnementstatus über RevenueCat).
- **Website-Besucher** auf öffentlichen Seiten für Erwachsene (Google Analytics 4 nach Einwilligung; das Kontaktformular über Formspree; Angebotsanfragen und Botschafterbewerbungen über den eigenen Server des Auftragsverarbeiters; die Dinner-Questions-E-Mails über Brevo).
- **Öffentliche Quiz-Bestenliste** (freiwillig: ein aus einer generierten Liste gewählter Spitzname, die Punktzahl und ein schlüsselbasierter Hash der IP-Adresse; 30 Tage gespeichert).
- **Programmumfragen,** die der Auftragsverarbeiter außerhalb einer Klasse durchführt, mit Einwilligung eines Elternteils, wo das Gesetz dies verlangt.
- **Eigenständige Dienste:** Die Eco Heroes Academy (learn.eco-heroes.org) und das VSME-Assessment (assessment.eco-heroes.org) haben eigene Bedingungen und Datenschutzhinweise.

C. Aufbewahrungsplan (wie im Dienst umgesetzt)

Anhang I.C — Aufbewahrungsplan

Daten	Aufbewahrung	Mechanismus
Daten von Schülerinnen und Schülern sowie von Kindern in Unternehmens- und Hotelgruppen (Spitzname, Altersgruppe, Avatar, Fortschritt, Aufgaben, Klassenaktivität in der App, LTI-Platzzuordnung)	Während der Lizenz: bis eine Lehrkraft oder ein Administrator die Schülerin, den Schüler oder die Klasse löscht. Nach dem Ende der Lizenz: Löschung 90 Tage nach dem Enddatum, sofern die Lizenz nicht verlängert wird. Auf schriftliches Verlangen des Verantwortlichen: Löschung innerhalb von 30 Tagen; die Schuladministratoren werden 30 und 7 Tage vor der Löschung per E-Mail benachrichtigt	Handlung der Lehrkraft oder des Administrators im Dienst; automatische Löschung zum Lizenzende; der Auftragsverarbeiter auf schriftliches Verlangen
Aktivitätsdaten von Heldenprofilen in Unternehmens- und Hotelgruppen (Organisationsbericht)	Werden mit dem Heldenprofil gespeichert und nach der Regel oben mit ihm gelöscht	Löschung mit dem Profil

Daten	Aufbewahrung	Mechanismus
Einstellungen der Organisation: Teamnamen und Teamzuordnung der Gruppen, Einstellung der Team-Rangliste, Name und Logo für das Co-Branding, Konfiguration der Firmen-Anmeldung	Für die Laufzeit der Lizenz; Löschung auf Wunsch des Verantwortlichen	Auftragsverarbeiter auf Anfrage
Firmen-Anmeldung: Datensätze des Anmeldevorgangs; festgelegte Identitätsverknüpfungen (schlüsselbasierter Hash der Subjektkennung des Identitätsanbieters)	Datensätze des Anmeldevorgangs: gelöscht nach Verwendung oder nach 10 Minuten. Identitätsverknüpfungen: bis das Konto gelöscht oder die Anmeldekonfiguration des Verantwortlichen entfernt oder zurückgesetzt wird	Automatische Bereinigung; Aktion eines Administrators
Live-Klassenquiz (Spitznamen, Antworten, Zeiten, Punktzahlen)	30 Tage nach Anlage der Quiz-Sitzung	Automatische tägliche Bereinigung
Vorschauen von Klassenlisten-Importen (OneRoster)	30 Minuten, nur in der Server-Sitzung der Lehrkraft	Ablauf der Sitzung
Google-Classroom-Zugriffstoken (Klassenlisten-Import)	Nur während des Imports, in der Sitzung der Lehrkraft; nie in die Datenbank geschrieben	Ablauf der Sitzung
LTI-Startdatensätze	Starts von Lehrkräften und von Schülerinnen und Schülern ohne Bewertungsdienst: 2 Stunden. Starts von Schülerinnen und Schülern mit Bewertungsdienst: 90 Tage	Automatische Bereinigung bei LTI-Aktivität
LTI-Anmeldestatus, Übergabetoken, Deep-Linking-Token, Nonces, Klassenlisten-Importtoken	10 Minuten / 10 Minuten / 60 Minuten / 15 Minuten / 2 Stunden	Automatische Bereinigung; einmalige Verwendung
Konten von Lehrkräften, Koordinatoren und Schuladministratoren	12 Monate nach dem Ende der letzten mit dem Konto verbundenen Lizenz; kostenlose Konten nach 12 Monaten ohne Anmeldung; Warn-E-Mail 30 Tage vor der Löschung. Unbestätigte Registrierungen: Löschung 7 Tage nach Ablauf des letzten Bestätigungslinks	Automatische Kontenbereinigung
Sitzungen und „Angemeldet bleiben“	Server-Sitzung für ihre konfigurierte Dauer, erneuert bei der Anmeldung und alle 30 Minuten; alle Sitzungen enden bei einer Passwortänderung oder wenn ein Administrator den Zugang entzieht. „Angemeldet bleiben“-Cookie: 180 Tage (HMAC-signiert)	Code

Daten	Aufbewahrung	Mechanismus
Datensätze zur Ratenbegrenzung (Anmeldeversuche und andere Grenzen)	30 Tage	Automatische tägliche Bereinigung
Sicherheits-Audit-Protokoll (administrative Handlungen, Code-Aktivierungen und Anmeldungen; schlüsselbasierter Hash der IP, Land der Verbindung als 2-Buchstaben-Code)	12 Monate	Automatische tägliche Bereinigung
IP-Hashes zur Missbrauchsabwehr bei Umfrageantworten und Einwilligungsanfragen	30 Tage (die Antwort selbst folgt ihrer eigenen Frist)	Automatische tägliche Bereinigung
Anfragen zur elterlichen Einwilligung	Unbeantwortet oder abgelaufen: 30 Tage. Ablehnungen: 12 Monate. Erteilte Einwilligung: solange sie in Anspruch genommen wird; bei Widerruf zusammen mit den Daten gelöscht	Automatische tägliche Bereinigung; Löschfunktion
Antworten aus Wirkungsstudien (Schülerinnen und Schüler, Lehrkräfte, Beobachtungsbögen) und Widerspruchs- oder Einwilligungsvermerke	24 Monate nach Abschluss der letzten Befragungsrunde der Studie; früher auf schriftliche Weisung des Verantwortlichen. Widerspruchs- und Einwilligungsvermerke werden mit der Anmeldung der Klasse gelöscht	Automatische tägliche Bereinigung; der Auftragsverarbeiter auf schriftliches Verlangen
Kinderschutz-Hinweise (Antworten aus Wirkungsstudien, die einen Hinweis enthalten können, mit dem zugehörigen Platz und Spitznamen)	Der Text der Antwort wird 30 Tage, nachdem der Hinweis als erledigt markiert wurde, gelöscht; der Hinweis selbst 12 Monate nach der Erledigung	Automatische tägliche Bereinigung
Antworten auf Programmumfragen	24 Monate oder bis zum Widerruf der Einwilligung	Automatische tägliche Bereinigung; Löschfunktion
Einträge der öffentlichen Quiz-Bestenliste (nicht Gegenstand dieses Vertrags, der Vollständigkeit halber genannt)	30 Tage	Automatische tägliche Bereinigung
Nachweise der Annahme dieses Vertrags durch den Verantwortlichen (wer, wann, welche Version, schlüsselbasierter Hash der IP-Adresse; vom Auftragsverarbeiter als Verantwortlichem geführt, Klausel 13.3)	Für die Laufzeit der Lizenz und 6 Jahre nach ihrem Ende	Unterlagen des Auftragsverarbeiters

Daten	Aufbewahrung	Mechanismus
Nachweise der Zustimmung beim Bezahlvorgang sowie Kündigungs- und Widerrufserklärungen zu Familienangeboten (nicht Gegenstand dieses Vertrags, der Vollständigkeit halber genannt)	6 Jahre, mit den Buchhaltungsunterlagen (spanisches Handelsgesetzbuch, Artikel 30)	Buchhaltungsunterlagen
Aus einer Person abgeleiteter Zähler für die Teilnahmequote	2 Tage	Automatische tägliche Bereinigung
Telemetrie (Berichte über CSP-Verstöße und JavaScript-Fehler)	Keine Kennungen gespeichert (gekürzter User-Agent); Ratenzähler werden jede Minute zurückgesetzt; Protokoll auf 5 MB begrenzt	Code
Support-Korrespondenz (E-Mail)	Bis die Anfrage erledigt ist, höchstens 12 Monate nach der letzten Nachricht	Verfahren des E-Mail-Postfachs des Auftragsverarbeiters
Verschlüsselte Sicherungen	Verschlüsselte Sicherungen, rollierend aufbewahrt; gelöschte Daten verschwinden innerhalb von 14 Tagen aus allen Sicherungen	Automatisch
Ausweich-Replikat der Datenbank	Laufend; vollzieht jede Löschung nach	Replikation
Technische Protokolle des Webservers (IP-Adresse, aufgerufene Adresse)	Bis zu 90 Tage	Serverkonfiguration
Rechnungen und Zahlungsunterlagen	6 Jahre (spanisches Handelsgesetzbuch, Artikel 30); sie nennen die Kontaktpersonen des Verantwortlichen, niemals Schülerinnen oder Schüler	Buchhaltungsunterlagen

Anhang II — Technische und organisatorische Maßnahmen (Artikel 32 DSGVO)

Die zum Datum dieses Vertrags umgesetzten Maßnahmen. Sie werden mit jeder Version überprüft, und die aktuelle Zusammenfassung ist unter https://eco-heroes.org/trust/#security veröffentlicht. Der Auftragsverarbeiter kann die Maßnahmen aktualisieren, sofern das Gesamtschutzniveau nicht sinkt.

1. Verschlüsselung bei der Übertragung

- TLS 1.2 oder höher für alle Verbindungen; HTTP Strict Transport Security mit einem max-age von zwei Jahren, includeSubDomains und preload; automatische Zertifikatserneuerung; Origin-Zertifikate zwischen dem Content-Delivery-Netzwerk und den Servern.
- Die Anwendungsserver verbinden sich mit der Datenbank nur über TLS 1.2/1.3, mit Prüfung des Zertifikats gegen eine fest hinterlegte Zertifizierungsstelle; die Datenbank weist unverschlüsselte Verbindungen ab (require_secure_transport). Die Datenbankkonten sind auf die Anwendungs- und Ausweichhosts beschränkt.
- Sicherungen werden verschlüsselt (AES-256-CBC, PBKDF2 mit 200.000 Iterationen), bevor sie den Server verlassen, und werden nur über verschlüsselte Verbindungen übertragen. Es werden keine unverschlüsselten Archive geschrieben.

2. Schutz im Browser

- Content-Security-Policy: Inline-Skripte werden nur ausgeführt, wenn sie durch einen SHA-256-Hash je Skript oder auf einigen dynamischen Seiten durch eine Nonce je Anfrage freigegeben sind (kein unsafe-inline für Skripte — Inline-Stile bleiben erlaubt; object-src 'none', base-uri 'self', frame-ancestors 'none' außer für die LTI-Seiten, die nur registrierte Lernplattformen einbetten dürfen). Verstoßberichte werden mit Ratenbegrenzung erfasst. Seiten für Kinder laden keine Skripte Dritter. Auf Seiten für Erwachsene sind die einzigen Skripte Dritter Google Analytics nach Einwilligung und die Cloudflare-Turnstile-Prüfung auf Anmelde- und Registrierungsformularen.
- Webschriften werden auf dem eigenen Server des Auftragsverarbeiters gehostet. Es werden keine Anfragen an Google Fonts oder einen anderen Schriftanbieter gesendet.
- Sicherheits-Header: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy und Cross-Origin-Resource-Policy same-origin. Versions-Header von Server und PHP werden entfernt. HTTP TRACE und TRACK werden abgewiesen.
- Cookies: Das Sitzungscookie ist Secure, HttpOnly und SameSite=Strict, im strikten Sitzungsmodus; die Sitzungskennung ändert sich bei der Anmeldung, bei der Code-Aktivierung und alle 30 Minuten. Das „Angemeldet bleiben“-Cookie ist mit einem serverseitigen Schlüssel HMAC-signiert. Das LTI-Status-Cookie ist auf /lti/ beschränkt und partitioniert.
- Der Service Worker der Spiele speichert niemals Antworten mit no-store oder private oder Pfade für Mitglieder zwischen, sodass nach der Abmeldung keine geschützten Inhalte im Cache eines gemeinsam genutzten Geräts verbleiben.
- Antworten mit personenbezogenen Daten oder Inhalten für Mitglieder werden mit Cache-Control: private, no-store gesendet, und das Content-Delivery-Netzwerk speichert sie nie zwischen.

3. Zugriffskontrolle und Authentifizierung

- Persönliche Lehrkräftekonten: Ein Schulcode wird nur einmal verwendet, zur Anmeldung. Er legt ein persönliches Konto mit bestätigter E-Mail-Adresse an oder ordnet die Schule dem bestehenden Konto

der Lehrkraft zu. Danach meldet sich die Lehrkraft mit eigener E-Mail-Adresse und eigenem Passwort oder per Single Sign-on an. Ein Gerät, auf dem nur ein Schulcode eingegeben wurde, kann spielen, hat aber keine Lehrkräfte-Werkzeuge. Ein Administrator-Code richtet nur das erste Administratorkonto der Schule ein und ist verbraucht, sobald dieses Konto bestätigt ist; Lehrkräfte treten danach mit einem Personal-Code bei, den ein Schuladministrator im Dienst erstellt, der nur einmal angezeigt, nur als schlüsselbasierter Hash gespeichert und jederzeit ersetzt werden kann.

- Passwörter von Lehrkräften werden mit bcryptgehasht und in konstanter Zeit verglichen. Die E-Mail-Adresse muss vor der ersten Anmeldung bestätigt sein. Eine Passwortänderung beendet alle Sitzungen. Ein Schuladministrator kann einer Lehrkraft den Zugang sofort entziehen.
- Die Zwei-Faktor-Anmeldung (TOTP, mit gehashten Wiederherstellungscodes) ist für Schuladministratoren und die Super-Administratoren des Auftragsverarbeiters verpflichtend, und jede Lehrkraft sowie jede Koordinatorin und jeder Koordinator einer Unternehmens- oder Hotellizenz kann sie aktivieren. Der QR-Code für die Einrichtung wird auf dem Server erzeugt, sodass das Geheimnis den Server nie verlässt. Der zweite Faktor wird geprüft, bevor eine Sitzung entsteht, und Schuladministratoren müssen ihn überall dort verwenden, wo Schülerdaten sichtbar sind. Auch die Ansprechperson für Kinderschutz muss ihn verwenden, um Kinderschutz-Hinweise zu lesen. Nach 10 falschen Codes innerhalb von 24 Stunden wird der zweite Faktor des Kontos 15 Minuten lang gesperrt, und die Kontoinhaberin oder der Kontoinhaber wird per E-Mail informiert.
- Zugangscodes werden nur als schlüsselbasierte Hashes in einer Datei außerhalb des Web-Stammverzeichnisses gespeichert; der Schlüssel liegt außerhalb des Web-Stammverzeichnisses. Registrierungs- und Lizenzcodes werden ebenso gespeichert; ein Code wird einmal angezeigt, wenn er erstellt wird.
- Ratenbegrenzung bei Anmeldung (je IP-Adresse und je E-Mail/IP-Paar, mit einer globalen Obergrenze), Registrierung, Code-Einlösung, Klassenbeitritt, Beitritt zu einem Live-Quiz, Fortschrittssynchronisierung, Angebotsformular, LTI-Anmeldungen, Telemetrie-Endpunkten und Stripe-Rückgabeabfragen. CSRF-Token in jedem Formular, das Daten ändert. Schutz vor offenen Weiterleitungen bei jedem next=-Parameter.
- Serverseitig geprüfte Zugriffsrechte: Inhalte für Mitglieder (Missionsvideos, Quiz-Fragenpools, Bücher, LTI-Inhalte) werden nur ausgeliefert, nachdem serverseitig eine gültige Code-Sitzung, ein signierter gemerkter Code oder ein angemeldetes Konto geprüft wurde. Nichts, was der Browser selbst schreibt, gewährt Zugriff.
- Trennung nach Rolle und Schule: Jede Lehrkraft sieht nur ihre eigenen Klassen; Schuladministratoren sehen alle Klassen ihrer eigenen Schule und nichts von anderen Schulen; Lehrkräfte, die über LTI kommen, sehen nur die Klassen des Kurses, aus dem sie gestartet sind; Super-Administrator-Zugang ist auf namentlich benanntes Personal des Auftragsverarbeiters beschränkt.
- Alle Datenbankabfragen verwenden vorbereitete Anweisungen; kein exec, eval oder unserialize; Dateipfade werden nur aus Elementen einer Positivliste gebildet; Uploads (Klassenlisten als CSV/ZIP, Umfragebilder) sind größenbegrenzt, typgeprüft und werden außerhalb des Web-Stammverzeichnisses gespeichert; die Anzeige von PHP-Fehlern ist deaktiviert.
- Optionales Single Sign-on für die Mitarbeitenden von Unternehmen und Hotels über OpenID Connect (Authorization Code mit PKCE; signierte ID-Token, geprüft auf Aussteller, Empfänger, Ablauf und Nonce). Client-Geheimnisse werden verschlüsselt gespeichert. Konten werden nur innerhalb der zugelassenen E-Mail-Domains des Verantwortlichen zugeordnet und nie mit dem Konto einer anderen Organisation verknüpft.

4. Datenminimierung und Daten von Kindern

- Es werden keine E-Mail-Adressen, Nachnamen, Fotos, Geburtsdaten, Postanschriften, Standorte, Geräte- oder Werbekennungen von Schülerinnen und Schülern erhoben. Klassenlisten-Importe behalten den Vornamen und höchstens die ersten 3 Buchstaben des Nachnamens. Schülerinnen und Schüler, die über LTI kommen, werden unter einem schlüsselbasierten Hash der Nutzerkennung der Plattform mit Vorname und Initiale gespeichert; der Verantwortliche konfiguriert seine Plattform so, dass sie nur den Namen weitergibt.
- IP-Adressen werden nur als schlüsselbasierte Hashes (Präfix) gespeichert. Wer den Schlüssel besitzt, könnte sie wieder zuordnen; sie sind daher pseudonymisiert, nicht anonym. Wenn sie Inhalten beigefügt sind, werden sie nach 30 Tagen gelöscht.
- Seiten für Kinder (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books und ihre Sprachfassungen) laden keine Analyse und zeigen kein Einwilligungsbanner. Auf anderen Seiten wird die Analyse erst nach ausdrücklicher Einwilligung geladen.
- Missionsvideos für Mitglieder werden vom Auftragsverarbeiter gehostet und nach Prüfung der Zugriffsrechte ausgeliefert. Wo noch ein YouTube-Player verbleibt (freies Spiel), nutzt er youtube-nocookie.com und lädt erst, wenn die Nutzerin oder der Nutzer auf Wiedergabe tippt.
- Das Veröffentlichen in der öffentlichen Quiz-Bestenliste ist nach jedem Spiel freiwillig, unter einem generierten Spitznamen (ein Adjektiv und ein Tier; kein Freitext, keine Schulangabe). Die öffentliche Liste zeigt Spitzname und Punktzahl der besten 10 der letzten 30 Tage, und Einträge werden nach 30 Tagen gelöscht. Jede öffentliche Zeile hat einen Meldelink; eine dreimal gemeldete Zeile wird bis zur Prüfung ausgeblendet. Klassen-Bestenlisten sehen nur die Lehrkraft dieser Klasse und die Schuladministratoren, die Zeilen entfernen können.
- Freitextantworten werden beim Absenden automatisch gefiltert: E-Mail-Adressen und Telefonnummern werden entfernt, und Antworten, die auf eine kurze Liste von Wörtern passen, die auf eine Gefährdung eines Kindes hinweisen können, werden aus den Studiendaten genommen und nur an die Ansprechperson für Kinderschutz weitergegeben, die die Schule benannt hat. Namen werden nicht automatisch entfernt; die Forschenden, die die Antworten lesen, markieren mögliche Namen und nennen sie nie in Berichten. Ein möglicher Hinweis wird innerhalb eines Schultags an die von der Schule benannte Ansprechperson weitergegeben. Ist keine Ansprechperson für Kinderschutz benannt, treten die in Klausel 4.4 genannten Empfänger an ihre Stelle.
- E-Mail-Adressen von Eltern im Einwilligungsverfahren werden nie im Klartext gespeichert; es wird nur ein schlüsselbasierter Hash aufbewahrt.
- Organisationsberichte sind zusammengefasste Werte: Eine Zahl, die auf weniger als 5 Familien beruht, wird schon in der Berechnung ausgeblendet, sodass weder der Bildschirm noch die CSV sie zeigen kann. Nur die Administratoren der Organisation mit Zwei-Faktor-Anmeldung können sie öffnen; jeder Abruf und jeder Export ist in der Häufigkeit begrenzt und wird protokolliert.

5. Verfügbarkeit, Sicherung und Wiederherstellung

- Die folgenden Vorgänge laufen automatisch. Eine unabhängige Überwachung (UptimeRobot, 11 Prüfungen, alle 5 Minuten) alarmiert den Auftragsverarbeiter bei einem Fehler.
- Jede Nacht eine verschlüsselte Sicherung der Datenbank und der Anwendung; eine Kopie wird in einem getrennten Rechenzentrum in einem anderen EU-Land aufbewahrt. Jeden Monat wird automatisch eine Wiederherstellung getestet.
- Eine Sicherung vor jeder Version, mit einem getesteten Rückfallverfahren; die vorherige Produktivversion wird aufbewahrt.

- Ein Ausweichserver hält eine Kopie der Anwendung und ein laufendes Replikat der Datenbank. Fällt der Haupt-Webserver aus, leitet ein Lastausgleich mit Zustandsprüfung den Verkehr automatisch um; fällt der Datenbankserver aus, wird das Replikat nach einem geskripteten und geübten Verfahren hochgestuft. Beides wurde im Oktober 2026 getestet.
- Eine stündliche Infrastrukturprüfung (Zustand und Verzögerung des Replikats, Ablauf der Zertifikate, Speicherplatz, ausstehende Sicherheitsupdates, Adressbereiche des Content-Delivery-Netzwerks). Sicherheitsupdates des Betriebssystems werden automatisch installiert. Schutz vor DDoS-Angriffen und Bots am Netzrand.
- Die Staging-Umgebung ist von der Produktion getrennt (eigener Unix-Benutzer, PHP-Pool mit open_basedir, eigene Datenbankinstanz, Geheimnisse entfernt).

6. Protokollierung und Überwachung

- Sicherheitsereignisse (fehlgeschlagene Anmeldungen, Code-Einlösungen, administrative Handlungen, CSP-Verstoßberichte, Löschungen und Aufbewahrungsbereinigungen) werden mit schlüsselbasierten Hashes der IP-Adressen protokolliert. Das Sicherheits-Audit-Protokoll wird 12 Monate aufbewahrt, Datensätze zur Ratenbegrenzung 30 Tage (Anhang I Abschnitt C).
- Der aktuelle Dienststatus und jede Unterbrechung werden auf der öffentlichen Statusseite veröffentlicht.

7. Organisatorische Maßnahmen

- Der Zugang zu Produktivsystemen ist auf namentlich benannte Personen beschränkt. Jedes administrative Konto (Hosting, Datenbank- und Sicherungsserver, Content-Delivery-Netzwerk und DNS, Quellcode-Repository, Überwachung, E-Mail) verwendet die Zwei-Faktor-Anmeldung. Der Zugang zu den Servern erfolgt über SSH-Schlüssel. Firewalls beschränken den Zugang zur Datenbank und zum Ausweichserver auf die eigenen Hosts des Auftragsverarbeiters und die Adressbereiche des Content-Delivery-Netzwerks.
- Änderungen werden automatisch getestet (Continuous Integration; eine Version wird abgelehnt, wenn der Code die Tests nicht bestanden hat), durchlaufen zuerst die Staging-Umgebung und werden nach jeder Version in der Produktion geprüft (47 Live-Prüfungen). Eine statische Sicherheitsprüfung der Anwendung wird durchgeführt und dokumentiert (zuletzt: 16. Oktober 2026).
- Penetrationstest, Oktober 2026: ein strukturierter White-Box- und Grey-Box-Test der Plattform (Authentifizierung, Sitzungen, Zugriffskontrolle zwischen Schulen, Zahlungen, Offenlegung von Dateien und Daten, Ratenbegrenzung und Edge-Cache), durchgeführt vom eigenen Testteam des Auftragsverarbeiters. Alle kritischen, hohen und mittleren Befunde wurden vor der Freigabe behoben und erneut getestet. Ein externer Penetrationstest durch ein unabhängiges Unternehmen ist geplant.
- Ein Kanal zur Meldung von Sicherheitslücken ist unter /.well-known/security.txt veröffentlicht. Meldungen werden innerhalb von 5 Werktagen bestätigt, und kritische Probleme werden vor allen anderen Arbeiten behoben.
- Ein schriftliches Verfahren zur Behandlung von Vorfällen beschreibt, wie der Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten erkennt, eindämmt und dokumentiert und wie er die Meldefrist von 48 Stunden nach Klausel 9 einhält.
- Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungen, die er im Auftrag von Verantwortlichen durchführt (Artikel 30 Absatz 2 DSGVO), und eine Übermittlungsbewertung für jeden Unterauftragsverarbeiter außerhalb des EWR.
- Aufbewahrungsfristen sind im Code festgelegt, der sie umsetzt, sodass veröffentlichte und angewandte Frist nicht auseinanderfallen können.

- Geheimnisse (eingeschränkter Stripe-Schlüssel, Single-Sign-on-Zugangsdaten, Hash-Schlüssel) werden außerhalb des Web-Stammverzeichnisses aufbewahrt und nie in das Quellcode-Repository übernommen.

Anhang III — Unterauftragsverarbeiter und Dienste Dritter

Das Trust Centre (https://eco-heroes.org/trust/#subprocessors) zeigt dieselben beiden Listen.

Teil A — Unterauftragsverarbeiter, die Daten des Verantwortlichen verarbeiten

Anhang III.A — genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Tätigkeit	Ort	Garantie für die Übermittlung
Internet Girona, auf Infrastruktur von OVHcloud	Webhosting	Frankreich (EU)	In der EU; Standard-Datenverarbeitungsbedingungen des Anbieters
Hetzner Online GmbH, Gunzenhausen, Deutschland	Datenbank-Hosting, Ausweichserver und verschlüsselte Sicherungen	Deutschland und Finnland (EU)	In der EU; Standard-Datenverarbeitungsbedingungen von Hetzner
Cloudflare, Inc., San Francisco, USA	Content Delivery, TLS, Schutz vor Angriffen und Bots, Turnstile-Prüfung auf Anmelde- und Registrierungsformularen und automatisches Failover	Weltweites Edge-Netz; Ursprungsserver in der EU	Standard-Datenverarbeitungsbedingungen von Cloudflare mit den Standardvertragsklauseln (2021/914); EU-US-Datenschutzrahmen, sofern Cloudflare gelistet ist
Proton AG, Genf, Schweiz	Hosting der E-Mail info@ und security@eco-heroes.org: Support- und Datenschutzkorrespondenz mit dem Personal des Verantwortlichen	Schweiz	Angemessenheitsbeschluss der Europäischen Kommission für die Schweiz; Standard-Datenverarbeitungsbedingungen von Proton
Google (Google Ireland Ltd / Google LLC) — nur Anmeldung und Classroom-Import	Nur wenn der Verantwortliche sie aktiviert: Anmeldung der Lehrkräfte (Name, E-Mail-Adresse, Kennung; keine Schülerdaten); Import von Google-Classroom-Klassenlisten (Vor- und Nachname einmal gelesen und als Vorname mit Initiale gespeichert; das Zugriffstoken bleibt in der Sitzung der Lehrkraft)	EU / USA	Eigene Google-Bedingungen des Verantwortlichen; Standard-Datenverarbeitungsbedingungen von Google mit den Standardvertragsklauseln; EU-US-Datenschutzrahmen, sofern gelistet
Microsoft (Microsoft Ireland Operations Ltd) — nur Anmeldung	Nur wenn der Verantwortliche sie aktiviert: Anmeldung der Lehrkräfte (nur Identität; keine Schülerdaten)	EU / USA	Eigene Microsoft-Bedingungen des Verantwortlichen; Microsoft Products and Services DPA mit den Standardvertragsklauseln; EU-US-Datenschutzrahmen, sofern gelistet

Unterauftragsverarbeiter	Tätigkeit	Ort	Garantie für die Übermittlung
Google (YouTube, youtube-nocookie.com)	Wiedergabe ausgewählter Bildungsvideos, wo noch ein YouTube-Player verwendet wird: erweiterter Datenschutzmodus, lädt erst, wenn die Nutzerin oder der Nutzer auf Wiedergabe tippt	EU / USA	Bedingungen von Google; EU-US-Datenschutzrahmen, sofern gelistet
Moodle Pty Ltd (MoodleCloud), Westaustralien	Nur wenn der Verantwortliche die Eco-Heroes-Kursseite eco-heroes.moodlecloud.com statt seiner eigenen Lernplattform nutzt: Kurskonten auf dieser Seite und der Fortschritt, den die Spiele dorthin melden	MoodleCloud-Hosting auf Amazon Web Services	Datenverarbeitungsvereinbarung von MoodleCloud mit den Standardvertragsklauseln (2021/914) für jede Übermittlung außerhalb des EWR

Teil B — Dienste Dritter, die keine Daten des Verantwortlichen verarbeiten

Der Transparenz halber genannt. Soweit personenbezogene Daten betroffen sind, gilt die Datenschutzerklärung des Auftragsverarbeiters. Der eigene Mailserver des Auftragsverarbeiters versendet Konto-, Bestätigungs- und Service-E-Mails; er ist kein Dritter.

Anhang III.B — Dienste Dritter außerhalb dieses Vertrags

Dienst	Tätigkeit	Ort	Warum er nicht Gegenstand dieses Vertrags ist
Stripe	Kartenzahlungen für Familienabonnements auf der Website; der Auftragsverarbeiter liest Zahlungs- und Abonnementstatus	EU / USA; Datenverarbeitungsbedingungen von Stripe mit den Standardvertragsklauseln; EU-US-Datenschutzrahmen	Familienabonnenten sind eigene Kunden des Auftragsverarbeiters; es werden keine Schuldaten an Stripe gesendet
Google Analytics 4	Besuchsstatistiken auf öffentlichen Seiten für Erwachsene, nur nach Einwilligung; nie auf Seiten für Kinder oder im Lehrkräftebereich	EU / USA; Datenverarbeitungsbedingungen von Google mit den Standardvertragsklauseln; EU-US-Datenschutzrahmen	Es werden keine Daten des Verantwortlichen gesendet; der Auftragsverarbeiter ist für seine eigenen Webstatistiken verantwortlich
Formspree	Leitet Nachrichten aus dem allgemeinen Kontaktformular weiter	USA; Standard-Datenverarbeitungsbedingungen des Anbieters (Standardvertragsklauseln; EU-US-Datenschutzrahmen, sofern gelistet)	Die Nachrichten sind eigene Korrespondenz des Auftragsverarbeiters; nicht vom Dienst genutzt

Dienst	Tätigkeit	Ort	Warum er nicht Gegenstand dieses Vertrags ist
Brevo	Dinner-Questions-E-Mails für Familien (nach Anmeldung; nur E-Mail-Adresse)	EU	Newsletter für Familien; nicht vom Dienst genutzt
RevenueCat	Abonnementstatus in der App (nur Kontokennung und Kaufhistorie)	USA; Standardvertragsklauseln	Familienkonten der App; keine Schuldaten
Google Play / Apple App Store	Abonnementzahlungen in der App, vom Store eingezogen	EU / USA	Die Stores verkaufen das Abonnement als eigenständige Verantwortliche
Google / Apple (Anmeldung in der App)	Optionale Anmeldung der Eltern in der App (E-Mail-Adresse und Anmeldekennung)	EU / USA; EU-US-Datenschutzrahmen, Standardvertragsklauseln	Familienkonten der App; keine Schuldaten
UptimeRobot	Prüft, ob öffentliche Seiten und der Status-Endpunkt antworten	EU / USA	Verarbeitet keine personenbezogenen Daten

Anhang IV — Daten von Kindern

Dieser Anhang ergänzt die Anhänge I und II für Schülerinnen und Schüler unter 18 Jahren.

1. **Alter der digitalen Einwilligung.** Verlangt das für den Verantwortlichen geltende Recht für Dienste der Informationsgesellschaft, die einem Kind direkt angeboten werden, eine Einwilligung (Artikel 8 DSGVO), holt der Verantwortliche sie ein und dokumentiert sie. Dieses Alter beträgt 14 Jahre in Spanien (Artikel 7 LOPDGDD), 13 bis 16 Jahre in den anderen Mitgliedstaaten der EU und 13 Jahre im Vereinigten Königreich; für Schulen in den Vereinigten Staaten siehe Anhang V. Stützt sich der Verantwortliche für die schulische Nutzung auf eine andere Rechtsgrundlage, etwa eine Aufgabe im öffentlichen Interesse, ist keine Einwilligung erforderlich, und der Verantwortliche informiert Schülerinnen, Schüler und Eltern. Der Dienst prüft das Alter nicht. Seine beiden Altersgruppen (9–12 und 13–17) wählen nur Inhalte und die Videofassung aus.
2. **Einwilligungsverfahren für Eltern auf der Website.** Benötigt eine Funktion der Website die Einwilligung eines Elternteils für ein Kind unter dem Alter der digitalen Einwilligung, speichert der Dienst nichts, bevor der Elternteil über einen per E-Mail gesendeten Einmallink bestätigt hat. Gespeichert werden nur ein schlüsselbasierter Hash der E-Mail-Adresse des Elternteils, die Entscheidung und die Zeitstempel. Unbeantwortete Anfragen werden nach 30 Tagen gelöscht, Ablehnungen nach 12 Monaten. Ein Widerruf der Einwilligung löscht die auf ihrer Grundlage erhobenen Daten.
3. **Familienangebot.** Ein Elternteil oder Erziehungsberechtigter schließt das Familienabonnement ab und ist Kunde des Auftragsverarbeiters. Auf der Website verlangt der Bezahlvorgang von der kaufenden Person die Bestätigung, volljährig zu sein; in der App liegen Anmeldung und Kauf hinter einer Erwachsenenprüfung (eine einzutippende Rechenaufgabe). Keines von beiden ist eine Identitäts- oder Altersprüfung. Kinder eröffnen keine Konten auf der Website. Ein Kind kann einen Familiencode unter der Verantwortung seiner Eltern nutzen; daran sind keine Daten einer Schule geknüpft.
4. **Kein Profiling und keine Werbung.** Der Auftragsverarbeiter zeigt keine Werbung und verwendet keine Werbekennungen oder Werbe-SDKs. Er erstellt keine Schülerprofile über die Fortschrittsverfolgung hinaus, die die Lehrkräfte des Verantwortlichen sehen, trifft keine automatisierten Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung und verkauft oder teilt Schülerdaten niemals für Werbung.
5. **Keine Analyse auf Seiten für Kinder.** Seiten für Kinder (das Abenteuerspiel, der Spielebereich, das Quiz, die Bibliothek, die Zielseiten, Wordle, die Missionen und die Bücher, in allen 13 Sprachen) laden keine Analyse, keine Tracker und kein Einwilligungsbanner. Sie verwenden nur den unbedingt erforderlichen Browserspeicher (Sprache, Fortschritt auf dem Gerät, Sitzung).
6. **Wirkungsstudien.** Meldet der Verantwortliche Klassen für eine Wirkungsstudie an, antworten die Schülerinnen und Schüler im Unterricht im Rahmen der eigenen Bewertung des Unterrichts durch den Verantwortlichen. Der Verantwortliche informiert die Eltern im Voraus und gibt ihnen die Möglichkeit zu widersprechen, oder er holt eine schriftliche Einwilligung ein, wo sein Recht oder seine Regeln dies verlangen; der Dienst unterstützt beides und schließt die betreffenden Plätze aus. Schülerinnen und Schüler können jede Frage überspringen und werden auf dem ersten Bildschirm darauf hingewiesen. Lehrkräfte sehen nur Klassenergebnisse, und nur wenn mindestens 10 Schülerinnen und Schüler vorher und nachher geantwortet haben; keine Nutzerin und kein Nutzer der Schule sieht die einzelnen Antworten einer Schülerin oder eines Schülers. Eine Freitextantwort, die einen kinderschutzrelevanten Hinweis enthalten kann, wird an die vom Verantwortlichen benannte Ansprechperson weitergeleitet, die über das weitere Vorgehen entscheidet. Der Auftragsverarbeiter verwendet nur zusammengefasste, anonymisierte Ergebnisse nach Klausel 2.3, niemals Freitext. Ein möglicher Hinweis wird innerhalb

eines Schultags an die benannte Ansprechperson weitergegeben, und nur diese Person sieht ihn. Ist keine Ansprechperson für Kinderschutz benannt, treten die in Klausel 4.4 genannten Empfänger an ihre Stelle.

7. **Keine Kommunikationsfunktionen.** Der Dienst hat keinen Chat, keine Nachrichtenfunktion und keine öffentlichen Schülerprofile. Die öffentliche Quiz-Bestenliste ist freiwillig, verwendet nur Spitznamen aus einer generierten Liste, zeigt keinen Schulnamen, bewahrt Einträge 30 Tage auf und hat an jedem Eintrag einen Meldelink. Klassen-Bestenlisten sehen nur die Lehrkraft der Klasse und die Schuladministratoren, und ein dreimal gemeldeter öffentlicher Eintrag wird bis zur Prüfung ausgeblendet.
8. **Dem Verantwortlichen mitgeteiltes Restrisiko.** Eine Mitschülerin oder ein Mitschüler, die bzw. der einen Klassencode und den Spitznamen einer Schülerin oder eines Schülers kennt, kann deren Fortschritt auf einem anderen Gerät öffnen. Lehrkräfte können Schülerinnen und Schüler jederzeit sehen, umbenennen oder entfernen und den Klassencode erneuern. Der Verantwortliche berücksichtigt dies in seiner eigenen Bewertung und bei der Ausgabe der Klassencodes.
9. **Rechte von Eltern und Schülerinnen und Schülern.** Eltern sowie Schülerinnen und Schüler machen ihre Rechte gegenüber dem Verantwortlichen geltend. Die Lehrkräfte des Verantwortlichen können die Daten einer Schülerin oder eines Schülers direkt einsehen, exportieren, umbenennen, zurücksetzen und löschen. Der Auftragsverarbeiter leitet jede bei ihm eingehende Anfrage an den Verantwortlichen weiter (Klausel 8.2).
10. **Information für Kinder.** Der Auftragsverarbeiter veröffentlicht unter https://eco-heroes.org/legal/children/ einen Datenschutzhinweis für Kinder mit einem für Kinder geschriebenen Teil (Teil A) und einem Teil für Eltern und Schulen (Teil B). Der Verantwortliche kann ihn in seine eigenen Informationen für Schülerinnen, Schüler und Eltern übernehmen.

Anhang V — Verantwortliche im Vereinigten Königreich und in den Vereinigten Staaten

1. **Vereinigtes Königreich.** Hat der Verantwortliche seinen Sitz im Vereinigten Königreich, gelten Verweise dieses Vertrags auf die DSGVO als Verweise auf die UK GDPR und den Data Protection Act 2018, und die zuständige Aufsichtsbehörde ist das Information Commissioner's Office (ICO). Daten des Verantwortlichen werden auf Grundlage der britischen Angemessenheitsvorschriften für den EWR aus dem Vereinigten Königreich in den EWR übermittelt. Weiterübermittlungen in die Vereinigten Staaten stützen sich auf die britische Erweiterung des EU-US-Datenschutzrahmens, wenn der Anbieter zertifiziert ist, oder auf den UK International Data Transfer Addendum zu den Standardvertragsklauseln. Der Auftragsverarbeiter gestaltet den Dienst unter Berücksichtigung des Age Appropriate Design Code des ICO; seine Zusammenfassung der Umsetzung steht in Abschnitt 11 der Datenschutzerklärung.
2. **Vereinigte Staaten — FERPA.** Ist der Verantwortliche eine Schule oder ein Schulbezirk in den Vereinigten Staaten, die bzw. der dem Family Educational Rights and Privacy Act unterliegt, handelt der Auftragsverarbeiter als „school official“ mit einem berechtigten Bildungsinteresse im Sinne von 34 CFR 99.31(a)(1)(i)(B). Der Auftragsverarbeiter steht hinsichtlich der Verwendung und Pflege der Schülerakten unter der direkten Kontrolle des Verantwortlichen, verwendet sie nur für die Zwecke der Lizenz und gibt sie an niemanden weiter, außer an Unterauftragsverarbeiter nach Klausel 6 oder wenn das Gesetz es verlangt.
3. **Vereinigte Staaten — COPPA.** Für Schülerinnen und Schüler unter 13 Jahren kann der Verantwortliche anstelle der Eltern in die Erhebung der in Anhang I beschriebenen Daten einwilligen, wie es die Leitlinien der Federal Trade Commission zulassen, da die Daten nur für die Bildungszwecke

des Verantwortlichen und für keinen anderen kommerziellen Zweck verwendet werden. Der Verantwortliche hält die Eltern informiert und leitet ihre Anfragen auf Einsicht in die Daten ihres Kindes oder deren Löschung weiter; der Auftragsverarbeiter setzt sie nach Klausel 8 um.

4. **Vereinigte Staaten — Löschung und Meldung.** Für die Löschung am Ende der Lizenz gilt Klausel 10. Legt ein Gesetz eines Bundesstaats zum Schutz von Schülerdaten eine kürzere Frist für die Meldung von Verletzungen oder für die Löschung fest, hält der Auftragsverarbeiter sie ein, sobald der Verantwortliche ihm mitteilt, welches Gesetz gilt.
