이 문서는 편의를 위해 제공되는 번역본입니다. 법적 구속력이 있는 텍스트는 영어 버전이며, 차이가 있는 경우 영어 버전이 우선합니다. English (PDF)

데이터 처리 계약

규정(EU) 2016/679(GDPR) 제28조 및 개인정보 보호 및 디지털 권리 보장에 관한 12월 5일자 스페인 조직법 제 3/2018호(LOPDGDD) 제33조에 따라 — 라이선스 보유자(이하 "컨트롤러")와 Eco Heroes International SL(이하 "프로세서") 간에 체결함

당사자 및 역할

컨트롤러: _____ (라이선스에 기재된 학교, 학교 그룹, 교육 당국, 기업 또는 호텔의 명칭), 등록 주소 _____, 대표자 _____ (성명, 직위).
데이터 보호 사항에 관한 컨트롤러 연락처(관리 담당자 연락처 또는 지정된 경우 데이터 보호 책임자): _____.

프로세서: Eco Heroes International SL, CIF B44915940, 등록 사무소 17003 Girona(스페인), Registro Mercantil de Girona에 등기, 대표자 창업자 Karim Zouhdi. 데이터 보호 사항에 관한 연락처: info@eco-heroes.org, +34 690 814 215. 보안 신고: security@eco-heroes.org (https://eco-heroes.org/.well-known/security.txt 참조).

역할. 컨트롤러는 컨트롤러 데이터를 처리하는 목적과 방법을 결정하며, 그 데이터의 컨트롤러이다. 프로세서는 GDPR 제4조 제8호에 따른 프로세서로서 컨트롤러를 대신해서만 컨트롤러 데이터를 처리한다.

교사 계정. 각 교사는 본인 명의의 개인 계정을 가진다. 프로세서는 계정 자체(로그인, 보안, 2단계 인증 및 무료 교사용 자료)를 자체 개인정보 처리방침에 따라 컨트롤러로서 운영한다. 교사가 컨트롤러를 위하여 서비스 안에서 하는 모든 일은 컨트롤러 데이터이다. 즉, 컨트롤러 조직 내에서의 계정의 역할과 권한, 학급, 학생, 진행 상황, 과제, 실시간 퀴즈, 명단 가져오기, 학습 플랫폼에서의 실행 및 효과 연구가 이에 해당한다.

본 계약의 적용 범위 밖. 부속서 I 섹션 B에는 프로세서 자신이 컨트롤러인 처리가 열거되어 있다. 이는 프로세서의 개인정보 처리방침(https://eco-heroes.org/legal/privacy/)의 적용을 받으며 본 계약의 적용을 받지 아니한다. Eco Heroes Academy(learn.eco-heroes.org)와 VSME 평가(assessment.eco-heroes.org)는 자체 약관과 개인정보 안내를 가진 별도의 서비스이며, 본 계약은 이에 적용되지 아니한다.

본 계약은 라이선스의 일부를 구성한다. 개인정보 처리에 관하여 라이선스와 본 계약이 상충하는 경우 본 계약이 우선한다.

정의

- **"라이선스"**: 컨트롤러가 서비스를 이용하는 근거가 되는 계약으로서, 컨트롤러가 수락한 견적서 또는 주문서와 https://eco-heroes.org/legal/licence/ 에 게시된 학교 및 기관용 라이선스 조건으로 구성

된다.

- **“서비스”**: 제1.1조에 기술된 Eco Heroes 플랫폼 및 지원을 말한다.
- **“컨트롤러 데이터”**: 부속서 I 섹션 A에 기술된 바와 같이 프로세서가 본 계약에 따라 컨트롤러를 대신하여 처리하는 개인정보를 말한다.
- **“이용자”**: 컨트롤러가 서비스 이용을 허용한 학생, 교사, 학교 관리 담당자, 교직원, 직원, 투숙객 및 그 밖의 사람을 말한다.
- **“하위 프로세서”**: 프로세서가 컨트롤러 데이터를 처리하기 위하여 이용하는 다른 프로세서를 말한다.
- **“영업일”**: 월요일부터 금요일까지를 말하며, Girona(스페인)의 공휴일은 제외한다.
- GDPR 제4조에 정의된 용어(“개인정보”, “처리”, “개인정보 침해” 등)는 본 계약에서도 같은 의미를 가진다.

1. 대상 및 기간

1.1 프로세서는 라이선스에 따라 컨트롤러에게 서비스를 제공한다. 서비스에는 어드벤처 게임, 퀴즈, 단어 게임 및 실시간 학급 퀴즈, 그림책과 Story Library, 미션 영상, 안내서와 수업 활동지, 본인 명의의 교사 계정, 학급 관리와 과제, 선택적 명단 가져오기(CSV, OneRoster CSV, Google Classroom), Google 또는 Microsoft를 통한 선택적 교사 로그인, LTI 1.1 또는 LTI 1.3을 통한 컨트롤러의 학습 플랫폼과의 선택적 연동, 컨트롤러가 이용하는 경우 Eco Heroes 모바일 앱의 학급 대시보드, 선택적 효과 연구, 기업 및 호텔 라이선스의 경우 코디네이터 계정, 직원 또는 투숙객 자녀를 위한 접근 코드가 있는 그룹 및 그룹별 진행 보고서(CSV), 기관 집계 보고서, 기관 이름이 들어간 수료증, 컨트롤러 자체 ID 공급자를 통한 직원의 선택적 로그인, 그리고 지원이 포함된다.

1.2 프로세서는 라이선스 기간 동안, 그리고 제10조에 따라 모든 컨트롤러 데이터가 삭제되거나 반환될 때까지 컨트롤러 데이터를 처리한다.

2. 처리의 성격 및 목적; 범주

2.1 처리의 성격과 목적, 정보주체의 범주 및 개인정보의 범주는 **부속서 I**에 규정되어 있다.

2.2 프로세서는 컨트롤러에게 서비스를 제공하기 위한 목적으로만 컨트롤러 데이터를 처리한다. 프로세서는 컨트롤러 데이터를 광고, 서비스가 컨트롤러의 교사에게 보여 주는 학습 진행 상황을 넘어서는 학생 프로필 구축, 데이터의 판매 또는 대여, 또는 서비스 이외의 제품 개발에 사용하지 아니한다.

2.3 **익명화된 통계.** 컨트롤러가 학급을 효과 연구에 등록하는 경우, 컨트롤러는 프로세서에게 응답으로부터 집계 통계를 작성하도록 지시하며, 프로세서는 이를 자체 보고서와 출판물에 사용할 수 있다. 프로세서는 학생 10명 이상인 그룹의 응답만 집계하고, 자유 서술 응답은 결코 포함하지 아니하며, 어떠한 학생, 학급 또는 학교도 식별될 수 없음을 확인한다. 이와 같이 작성된 통계는 더 이상 개인정보가 아니다. 컨트롤러는 서면 통지로 언제든지 이 지시를 철회할 수 있으며, 그 이후에 수집된 응답은 컨트롤러 자신의 결과를 위해서만 사용된다.

3. 지시

3.1 프로세서는 제3국 또는 국제기구로의 이전에 관한 것을 포함하여 컨트롤러의 문서화된 지시에 따라서만 컨트롤러 데이터를 처리한다. 다만 프로세서가 적용받는 EU 법 또는 회원국 법이 처리를 요구하는 경우는 예외로 하며, 이 경우 프로세서는 해당 법이 중요한 공익을 이유로 그러한 통지를 금지하지 않는 한 처리 전에 그 법적 요건을 컨트롤러에게 통지한다.

3.2 컨트롤러의 문서화된 지시는 본 계약, 라이선스, 그리고 컨트롤러와 그 이용자가 서비스에서 선택하는 설정(예: 학급 생성, 명단 가져오기, 싱글 사인온 또는 학습 플랫폼 연동 활성화, 학급의 효과 연구 등록, 학생 또는 학급 삭제)이다. 그 밖의 지시는 컨트롤러의 관리 담당자 연락처가 서면으로 한다. info@eco-heroes.org 로 보내는 이메일로 충분하다.

3.3 프로세서는 어떤 지시가 GDPR, LOPDGDD 또는 그 밖의 EU 법이나 회원국 법의 데이터 보호 규정을 위반한다고 판단하는 경우 즉시 컨트롤러에게 알린다. 프로세서는 컨트롤러가 해당 지시를 확인하거나 변경할 때까지 그 이행을 중단할 수 있다.

4. 컨트롤러의 의무

4.1 컨트롤러는 처리의 적법성(학생 데이터 처리의 법적 근거 포함), GDPR 제13조 및 제14조가 요구하는 정보를 정보주체(학생 및 해당하는 경우 그 부모 또는 보호자, 교사, 관리 담당자, 직원 및 투숙객)에게 제공하는 것, 디지털 동의 연령 미만의 학생에 대하여 컨트롤러에게 적용되는 법이 요구하는 동의를 받는 것(GDPR 제8조, LOPDGDD 제7조: 스페인에서는 14세), 그리고 컨트롤러와 그 이용자가 입력하는 데이터의 정확성에 대하여 책임을 진다.

4.2 컨트롤러는 이용자에게 닉네임, 학급 이름, 과제 메모, 실시간 퀴즈 닉네임 및 설문 응답 등 자유 서술 입력란에 특수한 범주의 개인정보(GDPR 제9조), 성, 이메일 주소 또는 그 밖의 학생 직접 식별자를 입력하지 않도록 요청한다.

4.3 컨트롤러가 자체 학습 플랫폼(LTI) 또는 신원 제공자(싱글 사인온)를 연동하는 경우, 컨트롤러는 해당 시스템과 그 구성에 대하여 책임을 지며, 부속서 I에 기술된 데이터만 공유하도록 설정한다(LTI를 통한 학생의 경우 이름만 공유하고 이메일 주소는 공유하지 않는다).

4.4 컨트롤러는 관리 담당자 연락처를 지정하고, 효과 연구를 실시하기 전에 아동 보호(세이프가딩) 담당자를 지정하며, 두 연락처를 서비스 안에서 또는 프로세서에게 보내는 이메일로 최신 상태로 유지한다. 아동 보호 담당자가 지정되기 전까지, 또는 지정된 담당자의 계정이 닫혀 있는 동안 서비스는 아동 보호 알림을 컨트롤러의 학교 관리 담당자에게 전달한다. 서비스에서 학교에 연결되지 않은 학급(예: LTI 실행으로만 사용하는 학급)의 경우, 알림은 프로세서의 아동 보호 책임자에게 전달되며, 그 책임자는 이를 지체 없이 컨트롤러의 관리 담당자 연락처에 전달한다.

5. 프로세서의 의무

프로세서는 다음을 수행한다.

a. 제3조에 따라서만 컨트롤러 데이터를 처리한다.

b. 컨트롤러 데이터를 처리하도록 승인된 사람이 비밀유지를 약속하였거나 적절한 법정 비밀유지 의무를 지도록 보장하고, 운영 시스템에 대한 접근을 이를 필요로 하는 지정된 사람으로 제한한다.

c. **부속서 II**의 기술적·관리적 조치를 시행하고, 정보주체에 아동이 포함된다는 점을 고려하여 GDPR 제32조에 따라 위험에 적합한 보안 수준을 유지한다.

d. 제6조의 조건에 따라서만 다른 프로세서를 이용한다.

e. 처리의 성격을 고려하여, 가능한 범위에서 적절한 기술적·관리적 조치를 통해 정보주체의 권리 행사 요청(GDPR 제12조부터 제23조까지)에 응할 컨트롤러의 의무 이행을 제8조에 규정된 바에 따라 지원한다.

f. 처리의 성격과 프로세서가 이용할 수 있는 정보를 고려하여 GDPR 제32조부터 제36조까지(보안, 침해 통지, 데이터 보호 영향평가, 사전 협의)의 준수를 보장하도록 컨트롤러를 지원한다. 프로세서의 현행 데이터 보호 영향평가 요약은 트러스트 센터에 게시되어 있으며, 전체 평가는 요청 시 컨트롤러에게 제공된다.

g. 서비스 종료 시 컨트롤러의 선택에 따라 모든 컨트롤러 데이터를 삭제하거나 반환하고, EU 법 또는 회원국 법이 데이터의 보존을 요구하지 않는 한 기존 사본을 삭제한다(제10조).

h. GDPR 제28조의 준수를 입증하는 데 필요한 모든 정보를 컨트롤러에게 제공하고, 컨트롤러 또는 컨트롤러가 위임한 감사인이 수행하는 감사(현장 점검 포함)를 허용하고 이에 협력한다(제11조).

i. 컨트롤러를 대신하여 수행하는 모든 범주의 처리 활동에 대한 기록을 유지한다(GDPR 제30조 제2항).

j. 제7조의 조건에 따라서만 컨트롤러 데이터를 제3국으로 이전한다.

6. 하위 프로세서

6.1 컨트롤러는 **부속서 III 파트 A**에 열거된 하위 프로세서에 대하여 일반적인 서면 승인을 한다.

6.2 프로세서는 하위 프로세서의 추가 또는 교체를 계획하는 경우 최소 **30일** 전에 컨트롤러의 관리 담당자 연락처로 이메일을 보내고 https://eco-heroes.org/trust/ 를 갱신하여 컨트롤러에게 알린다. 컨트롤러는 데이터 보호에 관한 합리적인 사유로 이의를 제기할 수 있다. 통지 기간 내에 이의가 해결되지 않으면 컨트롤러는 위약금 없이 라이선스의 해당 부분을 해지할 수 있으며, 이 경우 제10조가 적용된다.

6.3 프로세서는 각 하위 프로세서를 해당 제공자의 표준 데이터 처리 조건에 따라 이용한다. 이 조건은 GDPR 제28조 제4항이 요구하는 바와 같이 적절한 기술적·관리적 조치에 관하여 충분한 보장을 제공하는 데이터 보호 의무를 하위 프로세서에게 부과한다. 프로세서는 각 하위 프로세서가 이러한 의무를 이행하는 것에 대하여 컨트롤러에게 전적으로 책임을 진다.

6.4 **부속서 III 파트 B**에는 프로세서가 이용하지만 컨트롤러 데이터를 **처리하지 않는** 제3자 서비스가 열거되어 있다. 이들은 개인정보를 처리하지 않거나 프로세서 자신이 컨트롤러인 데이터만 처리한다. 투명성을 위하여 열거한 것이며, 본 계약에서 말하는 하위 프로세서가 아니다.

6.5 학습 플랫폼이나 Google 또는 Microsoft 환경과 같은 컨트롤러 자신의 시스템은 컨트롤러가 선택하고 관리한다. 이는 프로세서의 하위 프로세서가 아니다.

7. 국외 이전

7.1 컨트롤러 데이터는 유럽연합 내에서 호스팅되고 저장된다. 애플리케이션 서버는 프랑스(Internet Girona, OVHcloud 인프라)에, 데이터베이스, 암호화된 백업 및 예비 서버는 독일과 핀란드(Hetzner Online GmbH)에 있다. 콘텐츠 전송 네트워크(Cloudflare)는 캐시된 공개 페이지를 글로벌 네트워크에서 제공한다. 개인정보가 포함된 응답은 비공개 및 저장 불가(no-store)로 지정되어 있으며, 네트워크는 이를 캐시하지 아니한다.

7.2 프로세서는 다음의 경우를 제외하고는 컨트롤러 데이터를 유럽경제지역 밖으로 이전하지 아니하며, 어떠한 하위 프로세서에게도 이전하도록 허용하지 아니한다. (i) 목적지에 대하여 유럽연합 집행위원회의 적정성 결정이 있는 경우(스위스, 그리고 프로세서가 공식 목록에서 인증을 확인한 기관에 대하여는 EU-미국 데이터 프라이버시 프레임워크를 포함한다), 또는 (ii) 집행위원회 시행결정(EU) 2021/914로 채택된 표준계약조항(모듈 3, 프로세서 간, 또는 해당하는 경우 모듈 2)에 근거하고, 이전 영향평가 결과 필요하다고 판단되면 보완 조치를 함께 적용하는 경우. 부속서 III에는 각 하위 프로세서에 적용되는 보호조치가 기재되어 있다. 프로세서는 유럽경제지역 밖의 각 하위 프로세서에 대하여 서면 이전 영향평가를 보관하며, 요청 시 컨트롤러에게 제공한다.

7.3 Cloudflare, Inc.는 암호화된 연결을 네트워크의 엣지에서 종료하므로 그곳에서 요청 데이터(IP 주소, 요청된 주소, 헤더)를 처리한다. 프로세서는 표준계약조항을 포함한 Cloudflare의 표준 데이터 처리 조건에 의거하며, Cloudflare가 데이터 프라이버시 프레임워크 공식 목록에 등재되어 있는 경우 EU-미국 데이터 프라이버시 프레임워크에 의거한다.

7.4 Proton AG는 프로세서의 이메일을 스위스에서 호스팅한다. 스위스에 대하여는 유럽연합 집행위원회의 적정성 결정이 있다.

8. 정보주체의 권리에 관한 지원

8.1 교사는 서비스 안에서 직접 학생의 데이터를 열람하고, 내보내고(CSV), 이름을 바꾸고, 초기화하고, 삭제할 수 있으며, 학급 전체를 삭제할 수 있다. 각 교사는 자신의 학급만 볼 수 있고, 학교 관리 담당

자는 해당 학교의 모든 학급을 볼 수 있으며 교사의 접근 권한을 즉시 회수할 수 있다. 컨트롤러는 가능한 경우 이러한 기능을 사용하여 요청에 응한다.

8.2 서비스를 통해 요청에 응할 수 없는 경우, 프로세서는 서면 요청을 받은 날부터 **10영업일** 이내에 컨트롤러를 지원한다. 프로세서가 정보주체(부모 또는 보호자 포함)로부터 컨트롤러 데이터에 관한 요청을 직접 받은 경우, 프로세서는 그 요청의 내용에 답변하지 아니한다. 프로세서는 컨트롤러가 달리 지시하지 않는 한 부당한 지체 없이 정보주체를 컨트롤러에게 안내하고 컨트롤러에게 알린다.

9. 개인정보 침해

9.1 프로세서는 컨트롤러 데이터에 영향을 미치는 개인정보 침해를 인지한 후 부당한 지체 없이, 늦어도 **48시간** 이내에 컨트롤러에게 통지한다. 최초 통지에는 그 시점에 알려진 범위에서 GDPR 제33조 제3항이 요구하는 정보, 즉 침해의 성격, 영향을 받는 정보주체와 기록의 범주 및 대략적인 수, 예상되는 결과, 그리고 취하였거나 취할 예정인 조치가 포함된다. 프로세서는 정보가 확인되는 대로 단계적으로 보완한다.

9.2 프로세서는 침해의 조사, 억제 및 기록에 관하여 컨트롤러와 협력하고, 감독기관(스페인의 경우 Agencia Española de Protección de Datos)에 대한 신고 및 정보주체에 대한 통지에 관하여 컨트롤러를 지원한다. 프로세서는 사실관계, 영향 및 취한 시정 조치를 포함하여 모든 개인정보 침해를 기록한다.

9.3 프로세서는 컨트롤러의 관리 담당자 연락처로 이메일을 보내 통지한다. 누구든지 보안 취약점을 security@eco-heroes.org 로 신고할 수 있다. 신고는 5영업일 이내에 접수 확인되며, 중대한 문제는 다른 모든 작업보다 우선하여 수정된다.

10. 보존, 삭제 및 반환

10.1 **라이선스 기간 중.** 컨트롤러 데이터는 서비스 코드에 구현된 보존 규칙을 반영한 부속서 I 섹션 C의 계획에 따라 보존된다. 교사는 언제든지 학생 또는 학급을 삭제할 수 있으며, 삭제는 운영 중인 데이터베이스와 예비 복제본에 즉시 반영된다.

10.2 **내보내기.** 라이선스 기간 동안 및 제10.3조에 따른 삭제 시까지, 컨트롤러는 서비스 안에서 학급 및 진행 데이터를 CSV로 내보내거나, 구조화되고 통상적으로 사용되며 기계 판독이 가능한 형식으로의 내보내기를 프로세서에게 요청할 수 있다.

10.3 **라이선스 종료.** 라이선스가 종료되고 갱신되지 않는 경우, 프로세서는 종료일부터 **90일** 후에 컨트롤러 데이터를 삭제한다. 컨트롤러가 서면으로 요청하는 경우, 프로세서는 라이선스의 종료 여부와 관계없이 요청일부터 **30일** 이내에 컨트롤러 데이터를 삭제한다. 프로세서는 요청 시 삭제를 서면으로 확인한다. 삭제에 앞서 프로세서는 삭제일 30일 전과 7일 전에 컨트롤러의 학교 관리 담당자에게 해당 날짜와 라이선스 갱신 또는 데이터 내보내기 방법을 알리는 이메일을 보낸다. 삭제는 첫 번째 메일로부터 30일, 두 번째 메일로부터 7일이 지나기 전에는 이루어지지 않는다.

10.4 **교사 계정.** 교사 계정에 연결된 마지막 라이선스가 종료되면 해당 계정은 무료 교사 계정으로 유지된다. 그 사이에 교사가 새 라이선스에 연결되지 않는 한, 해당 라이선스 종료일부터 12개월 후에 계정이 삭제된다. 무료 계정은 12개월 동안 로그인이 없으면 삭제된다. 프로세서는 삭제 30일 전에 교사에게 이메일을 보낸다. 교사 계정이 유지된다고 하여 컨트롤러 데이터가 보존되는 것은 아니며, 컨트롤러 데이터는 제10.3조에 따라 삭제된다.

10.5 **백업 및 복제본.** 삭제된 데이터는 통상적인 주기에 따라 백업에서 사라진다. 암호화된 백업은 순환 방식으로 보관되므로, 삭제된 데이터는 **14일** 이내에 모든 백업에서 사라진다. 예비 서버의 읽기 전용 복제본은 모든 삭제를 지속적으로 반영한다. 백업은 운영 시스템의 손실을 복구하기 위해서만 복원되며, 복원으로 삭제된 데이터가 되살아나면 삭제가 다시 적용된다.

10.6 **법정 보존.** 프로세서는 라이선스 종료 후에는 EU 법 또는 회원국 법이 요구하는 범위와 기간에 한하여 개인정보를 보존한다. 예를 들어 스페인 상법(Código de Comercio) 제30조에 따라 청구서와 회계 기록을 6년간 보존한다. 이러한 기록은 컨트롤러의 연락 담당자를 식별하며 학생 데이터를 포함하지 아니한다. 프로세서는 이를 부속서 II에 따라 보호하며 다른 목적으로 사용하지 아니한다.

11. 감사 및 정보

11.1 프로세서는 요청이 있는 경우 계약 연도마다 1회를 한도로(다만 개인정보 침해 후 또는 미준수에 대한 문서화된 합리적 의심이 있는 경우에는 추가로) 본 계약의 준수를 입증하는 데 필요한 정보를 컨트롤러에게 제공한다. 여기에는 현행 보안 요약(https://eco-heroes.org/trust/#security), 현행 하위 프로세서 목록, 컨트롤러를 대신하여 수행하는 처리의 기록, 이전 영향평가, 데이터 보호 영향평가, 최근의 복원 테스트 및 장애 조치 훈련 결과, 그리고 실시한 보안 검토의 결과가 포함된다.

11.2 이러한 정보로 충분하지 않은 경우, 컨트롤러 또는 컨트롤러가 위임하고 비밀유지 의무를 지는 독립 감사인은 최소 **30일** 전에 통지하고, 통상적인 업무 시간 내에, 프로세서의 업무나 다른 고객에게 부당한 지장을 주지 않는 방식으로 프로세서의 관련 처리를 감사할 수 있다. 각 당사자는 자신의 비용을 부담한다. 프로세서는 감사인에게 합리적인 비밀유지 계약에 서명하도록 요구할 수 있으며, 다른 고객과 공유하는 시스템에 대한 접근을 준수 확인에 필요한 범위로 제한할 수 있다.

12. 책임

12.1 각 당사자는 GDPR 제82조에 따라 정보주체에게 책임을 진다. 당사자 간의 책임은 라이선스의 책임 조항에 따른다. 본 계약이나 라이선스의 어떠한 규정도 법이 제한을 허용하지 않는 경우(고의에 의한 책임 포함) 당사자의 책임을 제한하지 아니한다.

12.2 프로세서가 컨트롤러의 지시로 인하여 또는 컨트롤러가 제4조의 의무를 이행하지 않아 과징금이나 손해배상을 지급하여야 하는 경우, 컨트롤러는 그 원인이 미치는 범위에서 프로세서에게 이를 보상하며, 그 반대의 경우도 같다.

13. 기간, 준거법 및 관할

13.1 본 계약은 라이선스 개시일에 효력이 발생하며, 제10조에 따라 모든 컨트롤러 데이터가 삭제되거나 반환된 때에 종료한다. 제5조 (b), 제10조, 제11조 및 제12조는 필요한 기간 동안 계속 효력을 가진다.

13.2 본 계약은 스페인 법과 GDPR 및 LOPDGDD를 포함한 EU 법을 준거법으로 한다. Girona(스페인) 법원이 관할권을 가진다. 다만 컨트롤러가 공공기관으로서 또는 공공조달법에 따라 적용받는 강행규정과 GDPR 제79조에 따른 정보주체의 권리는 영향을 받지 아니한다. 부속서 V에는 영국 및 미국의 컨트롤러에 관한 규정이 추가되어 있다.

13.3 본 계약의 변경은 서면으로 하며, 이메일로 충분하다. 프로세서는 현행 서식을 https://eco-heroes.org/trust/ 에 게시한다. 서식의 새 버전은 컨트롤러의 동의 없이 서명된 계약을 변경하지 아니한다. 컨트롤러의 학교 관리 담당자는 본 계약을 온라인으로 수락할 수 있으며, 프로세서는 누가, 언제, 어느 버전을 수락하였는지와 사용된 IP 주소의 키 해시를 기록한다.

서명

컨트롤러를 위하여	프로세서를 위하여 — Eco Heroes International SL
성명, 직위	Karim Zouhdi, 창업자
날짜, 서명	날짜, 서명

부속서 I — 처리 내용

A. 컨트롤러를 대신한 처리(본 계약의 적용 대상)

부속서 I.A — 컨트롤러를 대신한 처리

항목	내용
대상	라이선스에 따라 컨트롤러의 이용자에게 서비스를 제공하는 것.
성격	데이터의 호스팅, 저장, 표시 및 삭제; 진행 상황 기록; 실시간 학급 퀴즈; 과제; 수료증; 학급 관리; 컨트롤러가 제공하는 명단의 선택적 가져오기(붙여 넣기 또는 CSV 업로드, OneRoster CSV 1.1/1.2, Google Classroom); Names and Role Provisioning(명단 가져오기) 및 Assignment and Grade Services(점수 반환)를 포함한 컨트롤러의 학습 플랫폼에서의 선택적 LTI 1.1 / LTI 1.3 실행; 컨트롤러의 선택에 따른 Google 또는 Microsoft를 통한 선택적 교사 로그인; 컨트롤러가 학급 코드를 배포하는 경우 Eco Heroes 모바일 앱의 학급 대시보드; 컨트롤러가 등록한 학급에서의 선택적 효과 연구 설문; 기업 및 호텔 라이선스의 경우 코디네이터 계정, 그룹 접근 코드 및 그룹별 진행 보고서(CSV); 지원. 기업 및 호텔 라이선스의 경우 추가로: 기관을 위한 집계 활동 보고(기관 보고서와 합계, 5가족 미만에 근거한 수치는 숨김) 및 선택적 팀 순위표; 아동 수료증에 기관 이름과 로고 표시; 컨트롤러 자체의 ID 공급자를 통한 직원의 선택적 로그인(OpenID Connect).
목적	라이선스가 정한 진행 기록, 보고 및 평가와 함께 유엔 지속가능발전목표에 기반한 지속가능성 교육을 제공하는 것. 효과 연구의 경우: 컨트롤러 자신의 수업 평가(컨트롤러의 교사를 위한 학급 결과) 및 제2.3조에 따른 익명화된 집계 통계. 그 밖의 목적은 없다.
정보주체의 범주	학생(게임은 9세부터 17세까지를 위해 설계되었으며 9~12세와 13~17세의 두 연령 그룹이 있다. 인쇄용 수업 활동지는 6세부터 16세까지를 대상으로 하며, 컨트롤러는 재량에 따라 더 어린 학생에게 서비스를 사용할 수 있다); 교사; 학교 관리 담당자; 동의 절차가 사용되는 경우에 한하여 부모 및 보호자; 기업 및 호텔 라이선스의 경우 직원 또는 투숙객의 자녀와 기관의 코디네이터.
개인정보 — 학생(웹사이트, 학급 내)	학생 또는 교사가 입력하는 이름 또는 닉네임(2~24자; 명단 가져오기의 경우 이름과 성의 첫 글자이며, 이름이 같은 두 학생을 구별하기 위한 경우에만 성의 처음 3글자까지 확장하고, 전체 성명은 사용하지 않는다); 게임에서 선택한 연령 그룹(9~12세 또는 13~17세); 정해진 세트 중에서 고른 아바타; 언어; 진행 상황(점수, 달성한 목표와 미션, 퀴즈 별, 주제별 응답 수와 정답 수); 완료한 과제; 참여일과 최근 활동일; 진행 상황을 저장하기 위해 학생의 기기에 저장되는 임의의 학급 토큰. 실시간 학급 퀴즈의 경우: 입력한 닉네임, 응답, 응답 시간 및 점수. 수집하지 않는 것: 이메일 주소, 성, 사진, 생년월일, 우편 주소, 위치, 기기 또는 광고 식별자.
개인정보 — 학생(LTI 실행)	플랫폼 사용자 식별자의 키 해시(학생을 자리에 연결하기 위한 것); 플랫폼이 성적 서비스 접근 권한을 부여한 경우에만 실행 기록에 90일간 저장되는 플랫폼 사용자 식별자(점수 반환에 필요); 닉네임으로 사용하는 이름과 성의 첫 글자; 강좌 식별자와 강좌명; 역할; 로캘; 마지막으로 제출한 점수. 이메일 주소와 전체 성명은 저장하지 아니하며, 컨트롤러는 이름만 공유하도록 자체 플랫폼을 설정한다.
개인정보 — 학생(모바일 앱, 학급 대시보드)	활동(플레이한 일일 게임, 날짜, 언어, 점수, 완료 여부, 소요 시간; 달성한 목표, 배지) 및 앱이 생성하는 임의의 설치 식별자의 단방향 해시. 학생은 생성된 별칭으로 교사에게 표시된다. 대시보드는 활동 중인 학생이 5명 미만인 학급에 대하여는 아무것도 표시하지 아니한다.

항목	내용
개인정보 — 학생(컨트롤러가 학급을 등록한 경우의 효과 연구)	연구 설문에 대한 응답(선택, 평가 및 선택적인 짧은 자유 서술), 설문 버전, 언어, 연령 그룹, 시작 및 제출 시각, 품질 지표. 이메일 주소와 전화번호는 수신 시 자유 서술에서 제거된다. 아동 보호와 관련된 털어놓음이 담겼을 수 있는 응답은 컨트롤러가 지정한 담당자에게 표시된다. 응답은 학급 내 학생 자리의 키 단방향 해시로 연구의 각 회차 사이에서 연결되며, 이름, 이메일 주소, 생년월일은 수집하지 아니한다. 자리별로 컨트롤러가 기록한 이의 또는 서면 동의. 아동 보호 담당자가 지정되지 않은 경우에는 제4.4조에 정한 수령인이 이를 대신한다.
개인정보 — 교사 및 학교 관리 담당자	성명, 업무용 이메일 주소, 학교, 역할(교사 또는 학교 관리 담당자), 언어; 비밀번호(bcrypt 해시) 또는 싱글 사인온 식별자; 활성화된 경우 2단계 인증 비밀값과 해시 처리된 백업 코드(학교 관리 담당자는 필수); 이메일 확인 상태; 로그인 시각과 횟수; 세션; 생성한 학급; 명단 가져오기 미리보기(이름만, 세션에 30분간 보관); 관리 작업 감사 로그 기록(IP 주소의 키 해시 및 콘텐츠 전송 네트워크가 제공하는 접속 국가의 2글자 코드 포함); 지원 관련 서신.
개인정보 — 교사(효과 연구)	교사 설문 응답 및 6~8세 아동의 경우 학급 관찰지로, 교사 계정 또는 코드의 키 단방향 해시로 연결된다; 학급의 등록, 동의 방식 및 연구 내 그룹 배정.
개인정보 — 부모 및 보호자	디지털 동의 연령 미만의 학생에 대하여 웹사이트의 보호자 동의 절차가 사용되는 경우에 한하여: 부모 이메일 주소의 키 단방향 해시(주소 자체는 확인 링크를 보내는 데 한 번 사용되며 저장되지 않는다), 결정 및 그 타임스탬프.
개인정보 — 자녀 및 코디네이터(기업 및 호텔 라이선스)	컨트롤러의 직원 또는 투숙객의 자녀: 자신의 기기나 가족 기기에서 컨트롤러의 접근 코드와 히어로 이름(닉네임)으로 그룹에 참여하며, 계정과 이메일 주소가 없다. 서비스는 학급 학생과 같은 데이터, 즉 히어로 이름, 연령 그룹, 아바타, 언어, 진행 상황 및 퀴즈 결과를 저장한다. 코디네이터: 성명, 업무용 이메일 주소, 비밀번호 해시 또는 로그인 식별자, 2단계 인증 설정 및 생성한 그룹. 코디네이터는 그룹별로 달성한 목표와 퀴즈 결과를 볼 수 있으며 이를 CSV로 내보낼 수 있다. 기관 보고서를 위해 본 서비스는 이 그룹들의 각 히어로 프로필에 대해 활동한 날과 각 목표·미션을 처음 완료한 날도 기록한다(일 단위; 학교 학급은 이렇게 기록하지 않음). 보고서에는 집계 값만 포함되며, 이름, 닉네임, 식별자, 아동별 행은 포함되지 않는다. 1~4가족에 근거한 수치는 숨기고(k = 5), 하나의 수치만으로 이를 추론할 수 있는 경우 두 번째 수치도 숨긴다. 팀 이름은 컨트롤러의 관리자가 정하며 개인을 지칭해서는 안 된다. 컨트롤러가 회사 계정 로그인을 사용하는 경우 직원의 이름과 이메일 주소는 컨트롤러 자체의 ID 공급자(범위 openid, email, profile)에서 받는다. 이 ID 공급자는 컨트롤러 자체의 시스템이자 프로세서이며 하위 프로세서가 아니고, 그 주체 식별자는 키 해시로만 저장한다. 공동 브랜딩: 컨트롤러가 제공하는 기관의 표시 이름과 로고. 보호자가 LinkedIn에 공유할 수 있는 공개 배지 페이지에는 개인정보가 없다(목표 수, 컨트롤러가 동의한 경우 기관 이름, 언어만 있으며 모두 링크에서 가져온다). 공유는 성인이 시작하며, 프로세서는 LinkedIn에 아무것도 보내지 않는다.
특수한 범주(GDPR 제9조)	요청하지 않으며 필요하지도 않다. 제4.2조 참조.
빈도	라이선스 기간 동안 지속적으로.

B. Eco Heroes가 독립적인 컨트롤러로서 수행하는 처리(본 계약의 적용 범위 밖)

본 계약의 범위가 어디까지인지 컨트롤러가 확인할 수 있도록 열거한다. 이는 프로세서의 개인정보 처리방침(v4.3) 및 아동 개인정보 안내(v2.2)의 적용을 받으며 본 계약의 적용을 받지 아니한다.

- **교사 계정 그 자체:** 로그인, 보안, 2단계 인증 및 무료 교사용 자료. 프로세서는 계정 자체의 컨트롤러이며 제10.4조에 따라 이를 삭제한다. 컨트롤러를 위한 계정의 활동은 컨트롤러 데이터이다.

- **무료 교사 계정:** 라이선스에 연결되지 않은 교사로서, 확인된 이메일 주소로 무료 교사용 자료(안내서 수업과 교사 가이드)를 이용하는 사람.
- **가족 구독** (웹사이트에서 부모 또는 보호자가 가입한 것): 이메일 주소(일부 마스킹하여 저장), Stripe 결제 및 구독 참조 정보, 개인 접근 코드(키 해시로 저장). 카드 정보는 프로세서에게 전달되지 않는다. 학교에서 사용하는 가족 코드는 학교 데이터를 전혀 수반하지 않는다.
- **앱 계정** (Google 또는 Apple을 통한 부모 로그인; Google Play 또는 Apple을 통한 구독; RevenueCat을 통한 구독 상태).
- **웹사이트 방문자** (성인용 공개 페이지: 동의 후 Google Analytics 4; Formspree를 통한 문의 양식; 프로세서 자체 서버를 통한 견적 요청 및 앰배서더 지원; Brevo를 통한 Dinner Questions 이메일).
- **퀴즈 공개 순위표** (선택 사항: 생성된 목록에서 고른 닉네임, 점수 및 IP 주소의 키 해시; 30일간 보관).
- **프로그램 설문:** 프로세서가 학급 밖에서 실시하는 것으로, 법이 요구하는 경우 부모의 동의를 받는다.
- **별도 서비스:** Eco Heroes Academy(learn.eco-heroes.org)와 VSME 평가(assessment.eco-heroes.org)는 자체 약관과 개인정보 안내를 가진다.

C. 보존 계획(서비스에 구현된 대로)

부속서 I.C — 보존 계획

데이터	보존	방식
학생 데이터 및 기업·호텔 그룹 자녀의 데이터(닉네임, 연령 그룹, 아바타, 진행 상황, 과제, 앱의 학급 활동, LTI 자리 연결)	라이선스 기간 중: 교사 또는 관리 담당자가 학생 또는 학급을 삭제할 때까지. 라이선스 종료 후: 라이선스가 갱신되지 않으면 종료일부터 90일 후 삭제. 컨트롤러의 서면 요청이 있는 경우: 30일 이내 삭제. 삭제 30일 전과 7일 전에 학교 관리 담당자에게 이메일로 통지	서비스에서의 교사 또는 관리 담당자의 조치; 라이선스 종료 시 자동 삭제; 서면 요청에 따른 프로세서의 조치
기업 및 호텔 그룹에 속한 히어로 프로필의 활동 날짜(기관 보고서)	히어로 프로필과 함께 보관하며 위 규칙에 따라 프로필과 함께 삭제	프로필과 함께 삭제
기관 설정: 팀 이름과 그룹별 팀 배정, 팀 순위표 설정, 공동 브랜딩 이름과 로고, 회사 계정 로그인 설정	라이선스 기간 동안; 컨트롤러의 요청 시 삭제	요청 시 프로세서가 처리
회사 계정 로그인: 로그인 절차 기록; 고정된 ID 연결(ID 공급자 주체의 키 해시)	절차 기록: 사용 시 또는 10분 후 삭제. ID 연결: 계정이 삭제되거나 컨트롤러의 로그인 설정이 제거·초기화될 때까지	자동 삭제; 관리자 조치
실시간 학급 퀴즈(닉네임, 응답, 시간, 점수)	퀴즈 세션 생성 후 30일	매일 자동 정리
명단 가져오기 미리보기 (OneRoster)	30분, 교사의 서버 세션 안에서만	세션 만료
Google Classroom 접근 토큰 (명단 가져오기)	가져오기 중에만, 교사의 세션 안에서; 데이터베이스에는 기록하지 않음	세션 만료
LTI 실행 기록	교사 실행 및 성적 서비스가 없는 학생 실행: 2시간. 성적 서비스가 있는 학생 실행: 90일	LTI 활동 시 자동 정리
LTI 로그인 상태, 인계 토큰, 딥 링크 토큰, 논스, 명단 가져오기 토큰	10분 / 10분 / 60분 / 15분 / 2시간	자동 정리; 1회 사용

데이터	보존	방식
교사, 코디네이터 및 학교 관리 담당자 계정	계정에 연결된 마지막 라이선스 종료 후 12개월; 무료 계정은 12개월간 로그인이 없을 경우; 삭제 30일 전 경고 이메일. 확인되지 않은 가입: 마지막 확인 링크 만료 7일 후 삭제	계정 자동 정리
세션 및 “로그인 상태 유지”	설정된 기간의 서버 세션으로, 로그인 시와 30분마다 갱신; 비밀번호 변경 시 또는 관리 담당자가 접근 권한을 회수할 때 모든 세션 종료. “로그인 상태 유지” 쿠키: 180일(HMAC 서명)	코드
속도 제한 기록(로그인 시도 및 그 밖의 제한)	30일	매일 자동 정리
보안 감사 로그(관리 작업, 코드 활성화, 로그인; IP 키 해시, 접속 국가의 2글자 코드)	12개월	매일 자동 정리
설문 응답 및 동의 요청에 대한 악용 방지용 IP 해시	30일(응답 자체는 고유한 기간을 따른다)	매일 자동 정리
보호자 동의 요청	미응답 또는 만료: 30일. 거부: 12개월. 부여된 동의: 이에 의거하는 동안; 동의가 철회되면 데이터와 함께 삭제	매일 자동 정리; 삭제 기능
효과 연구 응답(학생, 교사, 관찰지) 및 이의 또는 동의 표시	연구 마지막 회차 종료 후 24개월; 컨트롤러의 서면 지시가 있으면 그보다 일찍. 이의 및 동의 표시는 학급 등록과 함께 삭제	매일 자동 정리; 서면 요청에 따른 프로세서의 조치
아동 보호 알림(털어놓음이 담겼을 수 있는 효과 연구 응답과 그 응답이 속한 자리 및 닉네임)	응답 본문은 알림이 처리 완료로 표시된 후 30일에 삭제하고, 알림 기록은 처리 후 12개월에 삭제함	매일 자동 정리
프로그램 설문 응답	24개월 또는 동의가 철회될 때까지	매일 자동 정리; 삭제 기능
퀴즈 공개 순위표 기록(본 계약의 적용 범위 밖, 완전성을 위해 기재)	30일	매일 자동 정리
컨트롤러의 본 계약 수락 기록(수락한 사람, 시점, 버전, IP 주소의 키 해시; 프로세서가 컨트롤러로서 보관, 제13.3조)	라이선스 기간 동안 및 종료 후 6년	프로세서의 기록
가족 플랜의 결제 시 동의, 해지 및 철회 기록(본 계약의 적용 범위 밖, 완전성을 위해 기재)	회계 기록과 함께 6년(스페인 상법 제30조)	회계 기록
개인으로부터 도출된 참여율 카운터	2일	매일 자동 정리
원격 측정(CSP 위반 및 JavaScript 오류 보고)	식별자를 저장하지 않음(축약된 사용자 에이전트); 속도 카운터는 1분마다 초기화; 로그는 5 MB로 제한	코드
지원 관련 서신(이메일)	요청이 처리될 때까지, 그리고 마지막 메시지 후 최대 12개월	프로세서의 메일함 절차

데이터	보존	방식
암호화된 백업	암호화된 백업은 순환 방식으로 보관; 삭제된 데이터는 14일 이내에 모든 백업에서 사라짐	자동
데이터베이스 예비 복제본	지속적; 모든 삭제를 반영	복제
웹 서버 기술 로그(IP 주소, 요청된 주소)	최대 90일	서버 설정
청구서 및 결제 기록	6년(스페인 상법 제30조); 학생이 아니라 컨트롤러의 연락 담당자를 식별함	회계 기록

부속서 II — 기술적·관리적 조치(GDPR 제32조)

본 계약일 현재 시행 중인 조치이다. 각 릴리스 시 검토되며, 현행 요약은 https://eco-heroes.org/trust/#security 에 게시된다. 프로세서는 전반적인 보안 수준이 낮아지지 않는 한 조치를 갱신할 수 있다.

1. 전송 중 암호화

- 모든 연결에 TLS 1.2 이상 사용; max-age 2년, includeSubDomains 및 preload를 적용한 HTTP Strict Transport Security; 인증서 자동 갱신; 콘텐츠 전송 네트워크와 서버 간 오리진 인증서.
- 애플리케이션 서버는 고정된 인증 기관을 기준으로 인증서를 검증하는 TLS 1.2/1.3으로만 데이터베이스에 연결한다. 데이터베이스는 암호화되지 않은 연결을 거부한다(require_secure_transport). 데이터베이스 계정은 애플리케이션 호스트와 예비 호스트로 제한된다.
- 백업은 서버를 떠나기 전에 암호화되며(AES-256-CBC, 200,000회 반복 PBKDF2), 암호화된 연결로만 전송된다. 암호화되지 않은 아카이브는 기록되지 않는다.

2. 브라우저 보호

- Content-Security-Policy: 인라인 스크립트는 스크립트별 SHA-256 해시로 승인된 경우 또는 일부 동적 페이지에서 요청별 논스를 가진 경우에만 실행된다(스크립트에 unsafe-inline 없음 — 인라인 스타일은 계속 허용; object-src 'none', base-uri 'self', frame-ancestors 'none', 다만 등록된 학습 플랫폼만 삽입할 수 있는 LTI 페이지는 예외). 위반 보고는 속도 제한을 두고 수집된다. 아동용 페이지는 제3자 스크립트를 불러오지 않는다. 성인용 페이지에서 제3자 스크립트는 동의 후 Google Analytics와 로그인 및 가입 양식의 Cloudflare Turnstile 확인뿐이다.
- 웹 글꼴은 프로세서 자체 서버에서 호스팅된다. Google Fonts나 그 밖의 글꼴 제공자에게 요청을 보내지 않는다.
- 보안 헤더: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy 및 Cross-Origin-Resource-Policy same-origin. 서버 및 PHP 버전 헤더는 제거된다. HTTP TRACE와 TRACK은 거부된다.
- 쿠키: 세션 쿠키는 Secure, HttpOnly 및 SameSite=Strict이며 엄격 세션 모드를 사용한다. 세션 ID는 로그인 시, 코드 활성화 시 및 30분마다 변경된다. “로그인 상태 유지” 쿠키는 서버 측 키로 HMAC 서명된다. LTI 상태 쿠키는 /lti/로 제한되며 파티션화된다.
- 게임의 서비스 워커는 no-store 또는 private로 지정된 응답과 회원 전용 경로를 결코 캐시하지 않으므로, 공용 기기에서 로그아웃한 후 보호된 콘텐츠가 캐시에 남지 않는다.
- 개인정보나 회원 전용 콘텐츠가 포함된 응답은 Cache-Control: private, no-store로 전송되며, 콘텐츠 전송 네트워크는 이를 결코 캐시하지 않는다.

3. 접근 통제 및 인증

- 본인 명의의 교사 계정: 학교 코드는 가입을 위해 한 번만 사용된다. 학교 코드는 확인된 이메일 주소를 가진 본인 명의의 계정을 만들거나 교사의 기존 계정에 학교를 연결한다. 그 후 교사는 자신의 이메일 주소와 비밀번호 또는 싱글 사인온으로 로그인한다. 학교 코드만 입력한 기기는 게임을 할 수는 있지만 교사 도구는 사용할 수 없다. 관리자 코드는 학교의 첫 번째 관리 담당자 계정만 만들며, 그 계정이 확인되면 소진된다. 이후 교사는 학교 관리 담당자가 서비스에서 만드는 교직원 코드로 참여하며, 이 코드는 한 번만 표시되고 키 해시로만 저장되며 언제든지 교체할 수 있다.
- 교사의 비밀번호는 bcrypt로 해시되며 상수 시간으로 비교된다. 첫 로그인 전에 이메일 주소 확인이 필요하다. 비밀번호를 변경하면 모든 세션이 종료된다. 학교 관리 담당자는 교사의 접근 권한을 즉시 회수할 수 있다.

- 2단계 인증(해시 처리된 백업 코드가 있는 TOTP)은 학교 관리 담당자와 프로세서의 최고 관리자에게 필수이며, 모든 교사와 기업·호텔 라이선스의 코디네이터가 활성화할 수 있다. 등록용 QR 코드는 서버에서 생성되므로 비밀값이 서버 밖으로 나가지 않는다. 두 번째 요소는 세션이 생성되기 전에 확인되며, 학교 관리 담당자는 학생 데이터가 표시되는 모든 곳에서 이를 사용하여야 한다. 아동 보호 담당자도 아동 보호 알림을 읽으려면 이를 사용하여야 한다. 24시간 안에 잘못된 코드가 10번 입력되면 해당 계정의 두 번째 요소는 15분 동안 잠기며, 계정 소유자에게 이메일로 통지된다.
- 접근 코드는 웹 루트 밖의 파일에 키 해시로만 저장되며, 키는 웹 루트 밖에 보관된다. 가입 코드와 라이선스 코드도 같은 방식으로 저장된다. 코드는 생성 시 한 번만 표시된다.
- 로그인(IP 주소별, 이메일과 IP 조합별, 전체 한도 포함), 가입, 코드 사용, 학급 참여, 실시간 퀴즈 참여, 진행 상황 동기화, 견적 양식, LTI 로그인, 원격 측정 엔드포인트 및 Stripe 반환 조회에 속도 제한 적용. 데이터를 변경하는 모든 양식에 CSRF 토큰. 모든 next= 매개변수에 대한 오픈 리디렉션 방지.
- 접근 권한은 서버에서 확인된다. 회원 전용 자원(미션 영상, 퀴즈 문제 은행, 도서, LTI 콘텐츠)은 서버가 유효한 코드 세션, 서명된 기억된 코드 또는 로그인된 계정을 확인한 후에만 제공된다. 브라우저 스스로 기록하는 어떤 것도 접근 권한을 부여하지 않는다.
- 역할 및 학교별 분리: 각 교사는 자신의 학급만 볼 수 있고, 학교 관리 담당자는 해당 학교의 모든 학급을 볼 수 있으나 다른 학교의 것은 전혀 볼 수 없다. LTI로 들어온 교사는 실행한 강좌의 학급만 볼 수 있다. 최고 관리자 접근은 프로세서의 지정된 직원으로 제한된다.
- 모든 데이터베이스 쿼리는 준비된 구문(prepared statements)을 사용한다. exec, eval, unserialize는 사용하지 않는다. 파일 경로는 허용 목록의 요소로만 구성한다. 업로드(명단 CSV/ZIP 파일, 설문용 이미지)는 크기가 제한되고 형식이 확인되며 웹 루트 밖에 저장된다. PHP 오류 표시는 꺼져 있다.
- 기업 및 호텔 직원을 위한 선택적 싱글 사인온(OpenID Connect; PKCE를 사용하는 Authorization Code, 발급자·대상·만료·nonce를 검증하는 서명된 ID 토큰). 클라이언트 시크릿은 암호화하여 저장한다. 계정은 컨트롤러가 허용한 이메일 도메인 안에서만 연결되며, 다른 기관의 계정과는 절대 연결되지 않는다.

4. 데이터 최소화 및 아동 데이터

- 학생의 이메일 주소, 성, 사진, 생년월일, 우편 주소, 위치, 기기 또는 광고 식별자는 수집하지 않는다. 명단 가져오기는 이름과 성의 처음 3글자까지만 보관한다. LTI로 들어온 학생은 플랫폼 사용자 식별자의 키 해시와 이름 및 성의 첫 글자로 저장되며, 컨트롤러는 이름만 공유하도록 자체 플랫폼을 설정한다.
- IP 주소는 키 해시(접두부)로만 저장된다. 키를 가진 사람은 이를 다시 연결할 수 있으므로, 이는 익명이 아니라 가명 처리된 것이다. 콘텐츠에 수반되는 경우 30일 후 삭제된다.
- 아동용 페이지(/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books 및 그 언어별 버전)는 분석을 불러오지 않고 동의 배너도 표시하지 않는다. 그 밖의 페이지에서는 명시적인 동의 후에만 분석을 불러온다.
- 회원 전용 미션 영상은 프로세서가 호스팅하며 접근 권한을 확인한 후 제공된다. YouTube 플레이어가 남아 있는 곳(무료 플레이)에서는 youtube-nocookie.com을 사용하며, 이용자가 재생을 누를 때에만 불러온다.
- 퀴즈 공개 순위표 게시는 각 게임 후 선택하는 것이며, 생성된 닉네임(형용사와 동물; 자유 입력 없음, 학교 표시 없음)으로 이루어진다. 공개 순위표는 최근 30일간 상위 10명의 닉네임과 점수를 표시하며, 기록은 30일 후 삭제된다. 공개된 각 행에는 신고 링크가 있으며, 세 번 신고된 행은 검토될 때까지 숨겨진다. 학급 순위표는 해당 학급의 교사와 학교 관리 담당자만 볼 수 있으며, 이들은 행을 삭제할 수 있다.

- 자유 서술 응답은 전송될 때 자동으로 필터링된다. 이메일 주소와 전화번호는 제거되고, 아동이 위험에 처해 있음을 나타낼 수 있는 단어의 짧은 목록과 일치하는 응답은 연구 데이터에서 분리되어 학교가 지정한 아동 보호 담당자에게만 전달된다. 이름은 자동으로 제거되지 않으며, 응답을 읽는 연구자가 이름으로 보이는 것을 표시하고 보고서에서 이를 언급하지 않는다. 털어놓음일 수 있는 응답은 1수업일 이내에 학교가 지정한 담당자에게 전달된다. 아동 보호 담당자가 지정되지 않은 경우에는 제4.4조에 정한 수령인이 이를 대신한다.
- 동의 절차에서 부모의 이메일 주소는 평문으로 저장되지 않으며, 키 해시만 보관된다.
- 기관 보고서는 집계 값이다. 5가족 미만에 근거한 수치는 계산 단계에서 숨겨지므로 화면에도 CSV에도 나타나지 않는다. 2단계 인증으로 로그인한 기관 관리자만 열 수 있으며, 모든 조회와 내보내기는 횟수가 제한되고 기록된다.

5. 가용성, 백업 및 복구

- 다음 사항은 자동으로 실행된다. 독립적인 모니터링(UptimeRobot, 11개 점검, 5분마다)이 장애 시 프로세서에게 경고한다.
- 데이터베이스와 애플리케이션을 매일 밤 암호화하여 백업하고, 그 사본을 다른 EU 국가의 별도 데이터센터에 보관한다. 복원은 매달 자동으로 테스트한다.
- 각 릴리스 전에 백업을 수행하며, 테스트된 롤백 절차를 갖춘다. 이전 운영 버전은 보존된다.
- 예비 서버는 애플리케이션 사본과 데이터베이스의 실시간 복제본을 보유한다. 메인 웹 서버에 장애가 나면 상태 점검 기반 부하 분산이 트래픽을 자동으로 전환하고, 데이터베이스 서버에 장애가 나면 스크립트화되고 리허설을 마친 절차에 따라 복제본을 승격한다. 두 가지 모두 2026년 10월에 테스트했다.
- 매시간 인프라 점검(복제본 상태 및 지연, 인증서 만료, 디스크 공간, 대기 중인 보안 업데이트, 콘텐츠 전송 네트워크 주소 범위). 운영체제 보안 업데이트는 자동으로 적용된다. 네트워크 엣지에서 DDoS 공격 및 봇 방어.
- 테스트 환경은 운영 환경과 분리되어 있다(별도의 Unix 사용자, open_basedir를 적용한 PHP 풀, 별도의 데이터베이스 인스턴스, 비밀 정보 제거).

6. 로깅 및 모니터링

- 보안 이벤트(로그인 실패, 코드 사용, 관리 작업, CSP 위반 보고, 보존 기간에 따른 삭제 및 정리)는 IP 주소의 키 해시와 함께 기록된다. 보안 감사 로그는 12개월, 속도 제한 기록은 30일간 보관된다(부속서 I 섹션 C).
- 서비스의 현재 상태와 각 장애는 공개 상태 페이지에 게시된다.

7. 관리적 조치

- 운영 시스템에 대한 접근은 지정된 사람으로 제한된다. 모든 관리 계정(호스팅, 데이터베이스 및 백업 서버, 콘텐츠 전송 네트워크 및 DNS, 소스 코드 저장소, 모니터링, 이메일)은 2단계 인증을 사용한다. 서버 접근은 SSH 키로 한다. 방화벽은 데이터베이스와 예비 서버에 대한 접근을 프로세서 자체 호스트와 콘텐츠 전송 네트워크 주소 범위로 제한한다.
- 변경 사항은 자동으로 테스트되고(지속적 통합; 테스트를 통과하지 못한 코드의 릴리스는 거부됨), 먼저 테스트 환경을 거치며, 각 릴리스 후 운영 환경에서 확인된다(47개 실시간 점검). 애플리케이션의 정적 보안 검토를 실시하고 기록한다(최근: 2026년 10월 16일).
- 침투 테스트(2026년 10월): 프로세서 자체 테스트 팀이 플랫폼에 대해 화이트박스 및 그레이박스 방식의 체계적인 테스트를 수행했다(인증, 세션, 학교 간 접근 통제, 결제, 파일 및 데이터 노출, 속도 제한, 엣지 캐시). 심각·높음·중간 등급의 발견 사항은 모두 릴리스 전에 수정하고 다시 테스트했다. 독립 업체를 통한 외부 침투 테스트가 계획되어 있다.

- 취약점 신고 창구는 /.well-known/security.txt 에 게시되어 있다. 신고는 5영업일 이내에 접수 확인되며, 중대한 문제는 다른 모든 작업보다 우선하여 수정된다.
- 서면으로 된 사고 대응 절차는 프로세서가 개인정보 침해를 어떻게 탐지하고 억제하고 기록하는지, 그리고 제9조의 48시간 통지 기한을 어떻게 준수하는지를 규정한다.
- 프로세서는 컨트롤러를 대신하여 수행하는 처리의 기록(GDPR 제30조 제2항)과 유럽경제지역 밖의 각 하위 프로세서에 대한 이전 영향평가를 보관한다.
- 보존 기간은 이를 적용하는 코드 안에 정해져 있으므로, 공개된 기간과 적용되는 기간이 서로 다를 수 없다.
- 비밀 정보(제한된 Stripe 키, 싱글 사인온 자격 증명, 해시 키)는 웹 루트 밖에 보관되며 소스 코드 저장소에 들어가지 않는다.

부속서 III — 하위 프로세서 및 제3자 서비스

트러스트 센터(https://eco-heroes.org/trust/#subprocessors)에 같은 두 목록이 게시되어 있다.

파트 A — 컨트롤러 데이터를 처리하는 하위 프로세서

부속서 III.A — 승인된 하위 프로세서

하위 프로세서	수행 업무	위치	이전 보호조치
Internet Girona(OVHcloud 인프라)	웹 호스팅	프랑스(EU)	EU 내; 제공자의 표준 데이터 처리 조건
Hetzner Online GmbH, 군첸하우젠(독일)	데이터베이스 호스팅, 예비 서버, 암호화된 백업	독일 및 핀란드(EU)	EU 내; Hetzner의 표준 데이터 처리 조건
Cloudflare, Inc., 샌프란시스코(미국)	콘텐츠 전송, TLS, 공격 및 봇 방어, 로그인 및 가입 양식의 Turnstile 확인, 장애 시 자동 전환	글로벌 엣지 네트워크; 오리진 서버는 EU 내	표준계약조항(2021/914)을 포함한 Cloudflare의 표준 데이터 처리 조건; Cloudflare가 목록에 등재된 경우 EU-미국 데이터 프라이버시 프레임워크
Proton AG, 제네바(스위스)	info@ 및 security@eco-heroes.org 이메일 호스팅: 컨트롤러 직원과의 지원 및 데이터 보호 관련 서신	스위스	스위스에 대한 유럽연합 집행위원회의 적정성 결정; Proton의 표준 데이터 처리 조건
Google(Google Ireland Ltd / Google LLC) — 로그인 및 Classroom 가져오기만	컨트롤러가 활성화한 경우에만: 교사 로그인(성명, 이메일 주소, 식별자; 학생 데이터 없음); Google Classroom에서 명단 가져오기(이름과 성을 한 번 읽어 이름과 성의 첫 글자로 저장; 접근 토큰은 교사의 세션에 남음)	EU / 미국	컨트롤러 자신의 Google 약관; 표준계약조항을 포함한 Google의 표준 데이터 처리 조건; 목록에 등재된 경우 EU-미국 데이터 프라이버시 프레임워크
Microsoft(Microsoft Ireland Operations Ltd) — 로그인만	컨트롤러가 활성화한 경우에만: 교사 로그인(신원만; 학생 데이터 없음)	EU / 미국	컨트롤러 자신의 Microsoft 약관; 표준계약조항을 포함한 Microsoft Products and Services DPA; 목록에 등재된 경우 EU-미국 데이터 프라이버시 프레임워크
Google(YouTube, youtube-nocookie.com)	YouTube 플레이어가 아직 사용되는 일부 교육 영상의 재생: 개인정보 보호 강화 모드, 이용자가 재생을 누를 때에만 불러옴	EU / 미국	Google의 약관; 목록에 등재된 경우 EU-미국 데이터 프라이버시 프레임워크

하위 프로세서	수행 업무	위치	이전 보호조치
Moodle Pty Ltd(MoodleCloud), 서오스트레일리아	컨트롤러가 자체 학습 플랫폼 대신 Eco Heroes 강좌 사이트 eco-heroes.moodlecloud.com을 사용하는 경우에만: 해당 사이트의 강좌 계정 및 게임이 그곳에 보고하는 진행 상황	Amazon Web Services 기반 MoodleCloud 호스팅	유럽경제지역 밖으로의 모든 이전에 대하여 표준계약조항(2021/914)을 포함한 MoodleCloud의 데이터 처리 계약

파트 B — 컨트롤러 데이터를 처리하지 않는 제3자 서비스

투명성을 위하여 열거한다. 개인정보가 관련된 경우 프로세서의 개인정보 처리방침이 적용된다. 계정, 확인 및 서비스 관련 이메일은 프로세서 자체 메일 서버가 보내며, 이는 제3자가 아니다.

부속서 III.B — 본 계약의 적용 범위 밖의 제3자 서비스

서비스	수행 업무	위치	본 계약의 적용 범위 밖인 이유
Stripe	웹사이트 가족 구독의 카드 결제; 프로세서는 결제 및 구독 상태를 조회함	EU / 미국; 표준계약조항을 포함한 Stripe의 데이터 처리 조건; EU-미국 데이터 프라이버시 프레임워크	가족 구독자는 프로세서 자신의 고객이며, 학교 데이터는 Stripe로 전송되지 않음
Google Analytics 4	성인용 공개 페이지의 방문 통계, 동의 후에만; 아동용 페이지나 교사 영역에서는 사용하지 않음	EU / 미국; 표준계약조항을 포함한 Google의 데이터 처리 조건; EU-미국 데이터 프라이버시 프레임워크	컨트롤러 데이터는 전송되지 않음; 프로세서는 자체 웹 통계의 컨트롤러임
Formspree	일반 문의 양식의 메시지 전달	미국; 제공자의 표준 데이터 처리 조건(표준계약조항; 목록에 등재된 경우 EU-미국 데이터 프라이버시 프레임워크)	메시지는 프로세서 자신의 서신이며, 서비스에서 사용하지 않음
Brevo	가족을 위한 Dinner Questions 이메일(구독 후; 이메일 주소만)	EU	가족용 뉴스레터이며, 서비스에서 사용하지 않음
RevenueCat	앱 구독 상태(계정 식별자와 구매 내역만)	미국; 표준계약조항	앱 가족 계정; 학교 데이터 없음
Google Play / Apple App Store	앱 내 구독 결제, 스토어가 청구	EU / 미국	스토어는 독립적인 컨트롤러로서 구독을 판매함
Google / Apple(앱 로그인)	앱에서의 선택적 부모 로그인(이메일 주소와 로그인 식별자)	EU / 미국; EU-미국 데이터 프라이버시 프레임워크, 표준계약조항	앱 가족 계정; 학교 데이터 없음
UptimeRobot	공개 페이지와 상태 엔드포인트가 응답하는지 확인	EU / 미국	개인정보를 처리하지 않음

부속서 IV — 아동 데이터

본 부속서는 18세 미만 학생에 관하여 부속서 I 및 II를 보완한다.

1. **디지털 동의 연령.** 아동에게 직접 제공되는 정보사회 서비스에 대하여 컨트롤러에게 적용되는 법이 동의를 요구하는 경우(GDPR 제8조), 컨트롤러가 이를 받고 기록한다. 그 연령은 스페인에서 14세(LOPDGDD 제7조), 그 밖의 EU 회원국에서 13~16세, 영국에서 13세이며, 미국 학교에 관하여는 부속서 V를 참조한다. 컨트롤러가 학교에서의 이용을 공익 과업 등 다른 법적 근거에 기초하는 경우 동의는 필요하지 않으며, 컨트롤러가 학생과 부모에게 정보를 제공한다. 서비스는 연령을 확인하지 않는다. 두 연령 그룹(9~12세 및 13~17세)은 콘텐츠와 영상 버전을 선택하는 데에만 사용된다.
2. **웹사이트의 보호자 동의 절차.** 웹사이트의 기능이 디지털 동의 연령 미만의 아동에 대하여 부모의 동의를 필요로 하는 경우, 서비스는 이메일로 보낸 1회용 링크로 부모가 확인할 때까지 아무것도 저장하지 않는다. 부모 이메일 주소의 키 해시, 결정 및 타임스탬프만 저장된다. 미응답 요청은 30일 후, 거부는 12개월 후 삭제된다. 동의를 철회하면 그에 근거하여 수집된 데이터가 삭제된다.
3. **가족 플랜.** 부모 또는 보호자가 가족 구독에 가입하며 프로세서의 고객이 된다. 웹사이트에서는 결제 시 구매자에게 성년임을 확인하도록 요청하고, 앱에서는 로그인과 구매가 성인 확인(입력하는 계산 문제) 뒤에 있다. 어느 것도 신원 확인이나 연령 확인이 아니다. 아동은 웹사이트에서 계정을 만들지 않는다. 아동은 부모의 책임 아래 가족 코드를 사용할 수 있으며, 여기에는 학교 데이터가 연결되지 않는다.
4. **프로파일링 및 광고 없음.** 프로세서는 광고를 표시하지 않으며 광고 식별자나 광고 SDK를 사용하지 않는다. 컨트롤러의 교사가 보는 진행 기록을 넘어서는 학생 프로필을 구축하지 않고, 법적 효과 또는 이와 유사하게 중대한 영향을 미치는 자동화된 결정을 내리지 않으며, 학생 데이터를 광고 목적으로 판매하거나 공유하지 않는다.
5. **아동용 페이지에서 분석 없음.** 아동용 페이지(어드벤처 게임, 게임 모음, 퀴즈, 도서관, 목표 페이지, Wordle, 미션 및 도서, 13개 언어 모두)는 분석, 추적기, 동의 배너를 불러오지 않는다. 꼭 필요한 브라우저 내 저장(언어, 기기 내 진행 상황, 세션)만 사용한다.
6. **효과 연구.** 컨트롤러가 학급을 효과 연구에 등록하면, 학생은 컨트롤러 자신의 수업 평가의 일환으로 수업 중에 응답한다. 컨트롤러는 사전에 부모에게 알리고 이의를 제기할 기회를 주거나, 그 법이나 규정이 요구하는 경우 서면 동의를 받는다. 서비스는 두 방식을 모두 지원하며 해당 자리를 제외한다. 학생은 어느 질문이든 건너뛸 수 있으며 첫 화면에서 이를 안내받는다. 교사는 학급 결과만, 그리고 최소 10명의 학생이 사전과 사후에 모두 응답한 경우에만 볼 수 있으며, 학교의 어떤 이용자도 학생 개인의 응답을 보지 못한다. 아동 보호와 관련된 털어놓음이 담겼을 수 있는 자유 서술 응답은 컨트롤러가 지정한 담당자에게 전달되며, 그 담당자가 조치를 결정한다. 프로세서는 제2.3조에 따라 집계되고 익명화된 결과만 사용하며, 자유 서술은 결코 사용하지 않는다. 털어놓음일 수 있는 응답은 1수업일 이내에 지정된 담당자에게 전달되며, 그 담당자만 이를 볼 수 있다. 아동 보호 담당자가 지정되지 않은 경우에는 제4.4조에 정한 수령인이 이를 대신한다.
7. **소통 기능 없음.** 서비스에는 채팅, 메시지, 공개 학생 프로필이 없다. 퀴즈 공개 순위표는 선택 사항이며, 생성된 목록의 닉네임만 사용하고, 학교 이름을 표시하지 않으며, 기록을 30일간 보관하고, 각 기록에 신고 링크가 있다. 학급 순위표는 해당 학급의 교사와 학교 관리 담당자만 볼 수 있으며, 세 번 신고된 공개 기록은 검토될 때까지 숨겨진다.
8. **컨트롤러에게 알리는 잔여 위험.** 학급 코드와 학생의 닉네임을 아는 같은 반 친구는 다른 기기에서 그 학생의 진행 상황을 열 수 있다. 교사는 언제든지 학생을 보고, 이름을 바꾸고, 삭제할 수 있으며 학급 코드를 새로 발급할 수 있다. 컨트롤러는 자체 평가와 학급 코드 배포 방식에서 이를 고려한다.
9. **부모와 학생의 권리.** 부모와 학생은 컨트롤러에게 권리를 행사한다. 컨트롤러의 교사는 학생의 데이터를 직접 보고, 내보내고, 이름을 바꾸고, 초기화하고, 삭제할 수 있다. 프로세서는 받은 요청을 컨트롤러에게 전달한다(제8.2조).

10. **아동을 위한 안내.** 프로세서는 아동을 위해 쓴 부분(파트 A)과 부모 및 학교를 위한 부분(파트 B)으로 구성된 아동 개인정보 안내를 https://eco-heroes.org/legal/children/ 에 게시한다. 컨트롤러는 학생과 부모에게 제공하는 자체 안내에 이를 사용할 수 있다.

부속서 V — 영국 및 미국의 컨트롤러

1. **영국.** 컨트롤러가 영국에 설립된 경우, 본 계약에서 GDPR을 언급하는 것은 UK GDPR 및 Data Protection Act 2018을 언급하는 것으로 읽으며, 관할 감독기관은 Information Commissioner's Office(ICO)이다. 컨트롤러 데이터는 유럽경제지역에 관한 영국의 적정성 규정에 따라 영국에서 유럽경제지역으로 이전된다. 미국으로의 재이전은 제공자가 인증을 받은 경우 EU-미국 데이터 프라이버시 프레임워크의 영국 확장에, 그 밖의 경우 표준계약조항에 대한 UK International Data Transfer Addendum에 근거한다. 프로세서는 ICO의 Age Appropriate Design Code를 고려하여 서비스를 설계하며, 그 준수 요약은 개인정보 처리방침 제11절에 있다.
2. **미국 — FERPA.** 컨트롤러가 Family Educational Rights and Privacy Act의 적용을 받는 미국의 학교 또는 학군인 경우, 프로세서는 34 CFR 99.31(a)(1)(i)(B)에 따라 정당한 교육적 이익을 가진 “school official”로서 행위한다. 프로세서는 교육 기록의 사용 및 관리에 관하여 컨트롤러의 직접적인 통제를 받으며, 이를 라이선스의 목적으로만 사용하고, 제6조에 따른 하위 프로세서에게 제공하는 경우나 법이 요구하는 경우를 제외하고는 다른 사람에게 공개하지 않는다.
3. **미국 — COPPA.** 13세 미만 학생에 대하여 컨트롤러는 연방거래위원회 지침이 허용하는 바에 따라 부속서 I에 기술된 데이터의 수집에 부모를 대신하여 동의할 수 있다. 이는 데이터가 컨트롤러의 교육 목적으로만 사용되고 그 밖의 상업적 목적으로는 사용되지 않기 때문이다. 컨트롤러는 부모에게 계속 정보를 제공하며, 자녀의 데이터를 보거나 삭제해 달라는 부모의 요청을 전달한다. 프로세서는 제8조에 따라 이에 응한다.
4. **미국 — 삭제 및 통지.** 라이선스 종료 시의 삭제에는 제10조가 적용된다. 주(州)의 학생 개인정보 보호법이 침해 통지나 삭제에 대하여 더 짧은 기한을 정하는 경우, 프로세서는 컨트롤러가 어떤 법이 적용되는지 알리는 즉시 이를 준수한다.

Eco Heroes International SL · CIF B44915940 · 17003 Girona(스페인) · info@eco-heroes.org · https://eco-heroes.org/trust/ · 데이터 처리 계약 v1.7, 2026년 10월 25일. 게시된 서식은 검토용으로 제공되며, 서명된 버전이 라이선스의 일부가 된다.