Esta é uma tradução disponibilizada por conveniência. A versão inglesa é o texto juridicamente vinculativo e prevalece em caso de qualquer divergência. English (PDF)

Acordo de Subcontratação

nos termos do artigo 28.º do Regulamento (UE) 2016/679 (RGPD) e do artigo 33.º da Lei Orgânica espanhola 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDGDD) — entre o licenciado (o «Responsável pelo tratamento») e a Eco Heroes International SL (o «Subcontratante»)

Partes e funções

Responsável pelo tratamento: _____ (nome da escola, agrupamento de escolas, autoridade educativa, empresa ou hotel indicado na Licença), com sede em _____, representado por _____ (nome, cargo).
Contacto do Responsável pelo tratamento para a proteção de dados (contacto de administrador ou, se designado, encarregado da proteção de dados): _____.

Subcontratante: Eco Heroes International SL, CIF B44915940, com sede social em 17003 Girona (Espanha), inscrita no Registro Mercantil de Girona, representada por Karim Zouhdi, fundador. Contacto para a proteção de dados: info@eco-heroes.org, +34 690 814 215. Comunicações de segurança: security@eco-heroes.org (ver https://eco-heroes.org/.well-known/security.txt).

Funções. O Responsável pelo tratamento decide por que razão e de que forma os Dados do Responsável são tratados e é o responsável pelo seu tratamento. O Subcontratante trata os Dados do Responsável apenas por conta do Responsável pelo tratamento, na qualidade de subcontratante na aceção do artigo 4.º, ponto 8, do RGPD.

Contas de professor. Cada professor tem uma conta pessoal e nominativa. O Subcontratante gere a própria conta (início de sessão, segurança, autenticação de dois fatores e recursos gratuitos para professores) na qualidade de responsável pelo tratamento, nos termos da sua Política de Privacidade. Tudo o que um professor faz no Serviço para o Responsável pelo tratamento constitui Dados do Responsável: a função e os direitos da conta na organização do Responsável pelo tratamento, as turmas, os alunos, o progresso, os trabalhos, os quizzes ao vivo, as importações de listas de turma, os acessos a partir da plataforma de aprendizagem e os estudos de impacto.

Fora do presente Acordo. O Anexo I, secção B, enumera os tratamentos de que o próprio Subcontratante é responsável. Esses tratamentos regem-se pela Política de Privacidade do Subcontratante (https://eco-heroes.org/legal/privacy/), e não pelo presente Acordo. A Eco Heroes Academy (learn.eco-heroes.org) e a avaliação VSME (assessment.eco-heroes.org) são serviços distintos, com termos e informações de privacidade próprios; o presente Acordo não os abrange.

> O presente Acordo faz parte da Licença. Em caso de conflito entre a Licença e o presente Acordo em matéria de tratamento de dados pessoais, prevalece o presente Acordo.

Definições

- **«Licença»** designa o contrato ao abrigo do qual o Responsável pelo tratamento utiliza o Serviço: o orçamento ou a encomenda aceite pelo Responsável pelo tratamento, juntamente com os Termos de Licença para Escolas e Organizações publicados em https://eco-heroes.org/legal/licence/.
- **«Serviço»** designa a plataforma Eco Heroes e o apoio descritos na cláusula 1.1.
- **«Dados do Responsável»** designa os dados pessoais que o Subcontratante trata por conta do Responsável pelo tratamento ao abrigo do presente Acordo, descritos no Anexo I, secção A.
- **«Utilizadores»** designa os alunos, professores, administradores escolares, trabalhadores, pessoal, hóspedes e outras pessoas que o Responsável pelo tratamento autoriza a utilizar o Serviço.
- **«Subcontratante ulterior»** designa outro subcontratante a que o Subcontratante recorre para tratar Dados do Responsável.
- **«Dia útil»** designa de segunda a sexta-feira, excluindo os feriados em Girona (Espanha).
- Os termos definidos no artigo 4.º do RGPD, como «dados pessoais», «tratamento» e «violação de dados pessoais», têm o mesmo significado no presente Acordo.

1. Objeto e duração

1.1 O Subcontratante presta o Serviço ao Responsável pelo tratamento ao abrigo da Licença. O Serviço inclui: o jogo de aventura, o quiz, os jogos de palavras e os quizzes de turma ao vivo; os livros ilustrados e a Story Library, os vídeos das missões, os manuais e as fichas de aula; as contas de professor nominativas, a gestão de turmas e os trabalhos; a importação facultativa de listas de turma (CSV, CSV OneRoster, Google Classroom); o início de sessão facultativo dos professores com Google ou Microsoft; a ligação facultativa à plataforma de aprendizagem do Responsável pelo tratamento através de LTI 1.1 ou LTI 1.3; o painel de turma da aplicação móvel Eco Heroes, quando o Responsável pelo tratamento o utiliza; os estudos de impacto facultativos; nas licenças para empresas e hotéis, contas de coordenador, grupos com códigos de adesão para os filhos dos trabalhadores ou dos hóspedes e relatórios de progresso por grupo (CSV), um relatório agregado da organização, certificados com o nome da organização e início de sessão opcional do pessoal através do fornecedor de identidade do próprio Responsável pelo tratamento; e o apoio.

1.2 O Subcontratante trata os Dados do Responsável durante a vigência da Licença e até que todos os Dados do Responsável tenham sido apagados ou devolvidos nos termos da cláusula 10.

2. Natureza e finalidade do tratamento; categorias

2.1 O **Anexo I** descreve a natureza e a finalidade do tratamento, as categorias de titulares dos dados e as categorias de dados pessoais.

2.2 O Subcontratante trata os Dados do Responsável apenas para prestar o Serviço ao Responsável pelo tratamento. Não os utiliza para publicidade, para criar perfis de alunos que vão além do progresso de aprendizagem que o Serviço mostra aos professores do Responsável pelo tratamento, para vender ou alugar dados, nem para desenvolver um produto que não seja o Serviço.

2.3 **Estatísticas anonimizadas.** Quando o Responsável pelo tratamento inscreve turmas num estudo de impacto, dá instruções ao Subcontratante para elaborar estatísticas agregadas a partir das respostas,

que o Subcontratante pode utilizar nos seus próprios relatórios e publicações. O Subcontratante agrega apenas respostas de grupos de pelo menos 10 alunos, nunca inclui respostas de texto livre e verifica que nenhum aluno, turma ou escola pode ser identificado. As estatísticas assim elaboradas deixam de ser dados pessoais. O Responsável pelo tratamento pode retirar esta instrução a qualquer momento mediante aviso escrito; as respostas recolhidas posteriormente são utilizadas apenas para os resultados próprios do Responsável pelo tratamento.

3. Instruções

3.1 O Subcontratante trata os Dados do Responsável apenas mediante instruções documentadas do Responsável pelo tratamento, incluindo no que respeita às transferências para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito. Nesse caso, o Subcontratante informa o Responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se esse direito proibir tal informação por motivos importantes de interesse público.

3.2 São instruções documentadas do Responsável pelo tratamento o presente Acordo, a Licença e as definições que o Responsável pelo tratamento e os seus Utilizadores escolhem no Serviço (por exemplo, criar turmas, importar listas de turma, ativar o início de sessão único ou uma ligação a uma plataforma de aprendizagem, inscrever uma turma num estudo de impacto, apagar alunos ou turmas). O contacto de administrador do Responsável pelo tratamento dá quaisquer outras instruções por escrito; basta um e-mail para info@eco-heroes.org.

3.3 O Subcontratante informa imediatamente o Responsável pelo tratamento se, no seu entender, uma instrução violar o RGPD, a LOPDGDD ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados. O Subcontratante pode suspender a execução dessa instrução até que o Responsável pelo tratamento a confirme ou a altere.

4. Obrigações do Responsável pelo tratamento

4.1 O Responsável pelo tratamento é responsável pela licitude do tratamento, incluindo o fundamento jurídico para o tratamento dos dados dos alunos; pela prestação aos titulares dos dados das informações exigidas pelos artigos 13.º e 14.º do RGPD (alunos e, se for caso disso, os seus pais ou representantes legais, professores, administradores, trabalhadores e hóspedes); pela obtenção de qualquer consentimento que a lei aplicável ao Responsável pelo tratamento exija para alunos abaixo da idade de consentimento digital (artigo 8.º do RGPD; artigo 7.º da LOPDGDD: 14 anos em Espanha); e pela exatidão dos dados que ele e os seus Utilizadores introduzem.

4.2 O Responsável pelo tratamento pede aos seus Utilizadores que não introduzam categorias especiais de dados pessoais (artigo 9.º do RGPD), apelidos, endereços de e-mail ou outros identificadores diretos de alunos em campos de texto livre, como alcunhas, nomes de turma, notas de trabalhos, alcunhas dos quizzes ao vivo e respostas a inquéritos.

4.3 Quando o Responsável pelo tratamento liga a sua própria plataforma de aprendizagem (LTI) ou o seu fornecedor de identidade (início de sessão único), é responsável por esse sistema e pela sua configuração, de modo a que partilhe apenas os dados descritos no Anexo I (para os alunos através de LTI, apenas o nome e nunca o endereço de e-mail).

4.4 O Responsável pelo tratamento designa um contacto de administrador e, antes de realizar um estudo de impacto, um contacto para a proteção de crianças, e mantém ambos os contactos atualizados no Serviço ou por e-mail ao Subcontratante. Enquanto não for designado um contacto para a proteção de crianças, ou enquanto a conta do contacto designado estiver encerrada, o Serviço transmite os alertas

de proteção de crianças aos administradores escolares do Responsável pelo tratamento. Nas turmas que não estão ligadas a uma escola no Serviço (por exemplo, turmas usadas apenas através de um lançamento LTI), os alertas chegam ao responsável pela proteção de crianças do Subcontratante, que os transmite sem demora ao contacto de administrador do Responsável pelo tratamento.

5. Obrigações do Subcontratante

O Subcontratante:

a. trata os Dados do Responsável apenas nos termos da cláusula 3;

b. assegura que as pessoas autorizadas a tratar Dados do Responsável assumiram um compromisso de confidencialidade ou estão sujeitas a obrigações legais adequadas de confidencialidade, e que o acesso aos sistemas de produção está limitado a pessoas nominalmente identificadas que dele necessitam;

c. adota as medidas técnicas e organizativas do **Anexo II** e mantém um nível de segurança adequado ao risco nos termos do artigo 32.º do RGPD, tendo em conta que entre os titulares dos dados há crianças;

d. só recorre a outro subcontratante nas condições da cláusula 6;

e. tendo em conta a natureza do tratamento, presta assistência ao Responsável pelo tratamento através de medidas técnicas e organizativas adequadas, na medida do possível, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos (artigos 12.º a 23.º do RGPD), conforme previsto na cláusula 8;

f. presta assistência ao Responsável pelo tratamento no cumprimento dos artigos 32.º a 36.º do RGPD (segurança, notificação de violações, avaliação de impacto sobre a proteção de dados, consulta prévia), tendo em conta a natureza do tratamento e a informação ao seu dispor; o resumo da avaliação de impacto em vigor do Subcontratante está publicado no Trust Centre e a avaliação completa é disponibilizada ao Responsável pelo tratamento a pedido;

g. consoante a escolha do Responsável pelo tratamento, apaga ou devolve todos os Dados do Responsável depois de concluída a prestação do Serviço e apaga as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros (cláusula 10);

h. disponibiliza ao Responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento do artigo 28.º do RGPD e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo Responsável pelo tratamento ou por outro auditor por ele mandatado (cláusula 11);

i. conserva um registo de todas as categorias de atividades de tratamento realizadas por conta do Responsável pelo tratamento (artigo 30.º, n.º 2, do RGPD);

j. só transfere Dados do Responsável para um país terceiro nas condições da cláusula 7.

6. Subcontratantes ulteriores

6.1 O Responsável pelo tratamento dá uma autorização geral por escrito para os Subcontratantes ulteriores enumerados no **Anexo III, Parte A**.

6.2 O Subcontratante informa o Responsável pelo tratamento de qualquer inclusão ou substituição prevista de um Subcontratante ulterior com pelo menos **30 dias** de antecedência, por e-mail ao contacto de administrador do Responsável pelo tratamento e através da atualização de https://eco-heroes.org/trust/. O Responsável pelo tratamento pode opor-se por motivos razoáveis relacionados com a proteção de dados. Se a oposição não puder ser resolvida dentro do prazo de aviso, o Responsável pelo tratamento pode resolver a parte afetada da Licença sem penalização, aplicando-se a cláusula 10.

6.3 O Subcontratante recorre a cada Subcontratante ulterior ao abrigo dos termos normais de tratamento de dados desse fornecedor. Esses termos impõem ao Subcontratante ulterior obrigações de proteção de dados que apresentam garantias suficientes de execução de medidas técnicas e organizativas adequadas, como exige o artigo 28.º, n.º 4, do RGPD. O Subcontratante continua a ser plenamente responsável perante o Responsável pelo tratamento pelo cumprimento dessas obrigações por cada Subcontratante ulterior.

6.4 O **Anexo III, Parte B** enumera os serviços de terceiros que o Subcontratante utiliza mas que **não tratam** Dados do Responsável. Não tratam dados pessoais, ou tratam apenas dados de que o próprio Subcontratante é responsável. São enumerados por transparência e não são Subcontratantes ulteriores na aceção do presente Acordo.

6.5 Os sistemas próprios do Responsável pelo tratamento, como a sua plataforma de aprendizagem ou o seu ambiente Google ou Microsoft, são escolhidos e controlados pelo Responsável pelo tratamento. Não são Subcontratantes ulteriores do Subcontratante.

7. Transferências internacionais

7.1 Os Dados do Responsável são alojados e armazenados na União Europeia: os servidores de aplicações em França (Internet Girona, em infraestrutura OVHcloud); a base de dados, as cópias de segurança cifradas e um servidor de reserva na Alemanha e na Finlândia (Hetzner Online GmbH). A rede de distribuição de conteúdos (Cloudflare) serve páginas públicas em cache a partir da sua rede mundial. As respostas que contêm dados pessoais são marcadas como privadas e não armazenáveis (no-store), e a rede não as guarda em cache.

7.2 O Subcontratante não transfere Dados do Responsável para fora do Espaço Económico Europeu, nem permite que qualquer Subcontratante ulterior o faça, exceto (i) quando o destino beneficia de uma decisão de adequação da Comissão Europeia, incluindo a Suíça e, para as organizações cuja certificação o Subcontratante verificou na lista oficial, o Quadro de Privacidade de Dados UE-EUA; ou (ii) com base nas cláusulas contratuais-tipo adotadas pela Decisão de Execução (UE) 2021/914 da Comissão (módulo 3, de subcontratante para subcontratante, ou módulo 2, se for caso disso), complementadas por medidas suplementares quando uma avaliação da transferência demonstre que são necessárias. O Anexo III indica a garantia aplicável a cada Subcontratante ulterior. O Subcontratante mantém por escrito uma avaliação da transferência para cada Subcontratante ulterior fora do EEE e disponibiliza-a ao Responsável pelo tratamento a pedido.

7.3 A Cloudflare, Inc. termina a ligação cifrada na periferia da sua rede e trata aí, por conseguinte, dados de pedido (endereço IP, endereço pedido, cabeçalhos). O Subcontratante baseia-se nos termos normais de tratamento de dados da Cloudflare, que incluem as cláusulas contratuais-tipo e, quando a Cloudflare consta da lista oficial do Quadro de Privacidade de Dados, no Quadro de Privacidade de Dados UE-EUA.

7.4 A Proton AG aloja o correio eletrónico do Subcontratante na Suíça. A Suíça beneficia de uma decisão de adequação da Comissão Europeia.

8. Assistência no exercício dos direitos dos titulares

8.1 Os professores podem consultar, exportar (CSV), mudar o nome, repor e apagar os dados de um aluno, e apagar turmas inteiras, diretamente no Serviço. Cada professor vê apenas as suas próprias turmas; os administradores escolares veem todas as turmas da sua escola e podem retirar imediatamente o acesso a um professor. O Responsável pelo tratamento utiliza estas funções para responder aos pedidos sempre que possível.

8.2 Quando um pedido não puder ser satisfeito através do Serviço, o Subcontratante presta assistência ao Responsável pelo tratamento no prazo de **10 dias úteis** a contar de um pedido escrito. Se o Subcontratante receber diretamente de um titular dos dados (incluindo um pai, mãe ou representante legal) um pedido relativo a Dados do Responsável, não lhe responde quanto ao mérito. Encaminha o titular dos dados para o Responsável pelo tratamento sem demora injustificada e informa o Responsável pelo tratamento, salvo instrução em contrário deste.

9. Violação de dados pessoais

9.1 O Subcontratante notifica o Responsável pelo tratamento de qualquer violação de dados pessoais que afete Dados do Responsável sem demora injustificada e, o mais tardar, **48 horas** após ter tido conhecimento da mesma. A primeira notificação contém as informações exigidas pelo artigo 33.º, n.º 3, do RGPD na medida em que sejam conhecidas nesse momento: a natureza da violação, as categorias e o número aproximado de titulares e de registos afetados, as consequências prováveis e as medidas adotadas ou propostas. O Subcontratante completa essas informações de forma faseada à medida que forem ficando disponíveis.

9.2 O Subcontratante coopera com o Responsável pelo tratamento para investigar, conter e documentar a violação e presta-lhe assistência em qualquer notificação à autoridade de controlo (em Espanha, a Agencia Española de Protección de Datos) e em qualquer comunicação aos titulares dos dados. O Subcontratante documenta qualquer violação de dados pessoais, incluindo os factos, os respetivos efeitos e a medida de reparação adotada.

9.3 O Subcontratante envia as notificações por e-mail ao contacto de administrador do Responsável pelo tratamento. Qualquer pessoa pode comunicar uma vulnerabilidade de segurança para security@eco-heroes.org. As comunicações são confirmadas no prazo de 5 dias úteis e os problemas críticos são corrigidos antes de qualquer outro trabalho.

10. Conservação, apagamento e devolução

10.1 **Durante a Licença.** Os Dados do Responsável são conservados segundo o calendário do Anexo I, secção C, que reflete as regras de conservação aplicadas no código do Serviço. Um professor pode apagar um aluno ou uma turma a qualquer momento, com efeito imediato na base de dados ativa e na réplica de reserva.

10.2 **Exportação.** Durante a Licença, e até ao apagamento previsto na cláusula 10.3, o Responsável pelo tratamento pode exportar no Serviço os dados de turma e de progresso em formato CSV, ou pedir ao Subcontratante uma exportação num formato estruturado, de uso corrente e de leitura automática.

10.3 **Fim da Licença.** Se a Licença terminar e não for renovada, o Subcontratante apaga os Dados do Responsável **90 dias** após a data de termo. Se o Responsável pelo tratamento o pedir por escrito, o Subcontratante apaga os Dados do Responsável no prazo de **30 dias** a contar do pedido, quer a Licença tenha terminado quer não. O Subcontratante confirma o apagamento por escrito a pedido. Antes do apagamento, o Subcontratante envia um e-mail aos administradores escolares do Responsável pelo tratamento 30 dias e 7 dias antes da data de apagamento, indicando essa data e como renovar a Licença ou exportar os dados; o apagamento não ocorre antes de decorridos 30 dias desde a primeira mensagem e 7 dias desde a segunda.

10.4 **Contas de professor.** Quando termina a última licença associada a uma conta de professor, a conta continua como conta gratuita de professor. É apagada 12 meses após o termo dessa licença, salvo se entretanto o professor for associado a uma nova licença; uma conta gratuita é apagada após 12 meses sem início de sessão. O Subcontratante envia um e-mail ao professor 30 dias antes do apagamento. A

manutenção de uma conta de professor não conserva quaisquer Dados do Responsável: esses dados são apagados nos termos da cláusula 10.3.

10.5 **Cópias de segurança e réplica.** Os dados apagados saem das cópias de segurança no ciclo normal. As cópias de segurança cifradas são conservadas de forma rotativa, pelo que os dados apagados saem de todas as cópias de segurança no prazo de **14 dias**. A réplica só de leitura no servidor de reserva acompanha cada apagamento de forma contínua. As cópias de segurança só são restauradas para corrigir uma perda do sistema de produção; se um restauro repuser dados apagados, o apagamento é aplicado de novo.

10.6 **Conservação legal.** O Subcontratante só conserva dados pessoais após o termo da Licença na medida e pelo período exigidos pelo direito da União ou dos Estados-Membros, por exemplo faturas e registos contabilísticos durante 6 anos nos termos do artigo 30.º do Código Comercial espanhol (Código de Comercio). Esses registos identificam as pessoas de contacto do Responsável pelo tratamento e não contêm dados de alunos. O Subcontratante protege-os nos termos do Anexo II e não os utiliza para qualquer outra finalidade.

11. Auditoria e informação

11.1 A pedido, e no máximo uma vez por ano contratual (ou, adicionalmente, após uma violação de dados pessoais ou perante uma suspeita documentada e razoável de incumprimento), o Subcontratante faculta ao Responsável pelo tratamento as informações necessárias para demonstrar o cumprimento do presente Acordo. Estas incluem o resumo de segurança em vigor (https://eco-heroes.org/trust/#security), a lista em vigor de Subcontratantes ulteriores, o registo dos tratamentos realizados por conta do Responsável pelo tratamento, as avaliações das transferências, a avaliação de impacto sobre a proteção de dados, os resultados mais recentes dos testes de restauro e dos exercícios de comutação e os resultados de qualquer revisão de segurança.

11.2 Se essas informações não forem suficientes, o Responsável pelo tratamento, ou um auditor independente por ele mandatado e sujeito a confidencialidade, pode auditar os tratamentos relevantes do Subcontratante mediante aviso prévio de pelo menos **30 dias**, durante o horário de expediente e sem perturbação injustificada da atividade do Subcontratante ou de outros clientes. Cada parte suporta os seus próprios custos. O Subcontratante pode pedir ao auditor que assine um compromisso de confidencialidade razoável e limitar o acesso aos sistemas partilhados com outros clientes ao necessário para verificar o cumprimento.

12. Responsabilidade

12.1 Cada parte é responsável perante os titulares dos dados nos termos do artigo 82.º do RGPD. Entre as partes, a responsabilidade rege-se pela cláusula de responsabilidade da Licença. Nenhuma disposição do presente Acordo ou da Licença limita a responsabilidade de uma parte quando a lei não permita limitá-la, incluindo a responsabilidade por dolo.

12.2 Se o Subcontratante tiver de pagar uma coima ou uma indemnização devido às instruções do Responsável pelo tratamento ou porque este não cumpriu as suas obrigações nos termos da cláusula 4, o Responsável pelo tratamento indemniza o Subcontratante na medida dessa causa, e vice-versa.

13. Vigência, lei aplicável e foro

13.1 O presente Acordo entra em vigor na data de início da Licença e termina quando todos os Dados do Responsável tiverem sido apagados ou devolvidos nos termos da cláusula 10. As cláusulas 5(b), 10, 11 e 12 continuam a aplicar-se durante o tempo necessário.

13.2 O presente Acordo rege-se pelo direito espanhol e pelo direito da União Europeia, incluindo o RGPD e a LOPDGDD. São competentes os tribunais de Girona (Espanha), sem prejuízo das normas imperativas aplicáveis ao Responsável pelo tratamento enquanto entidade pública ou ao abrigo do direito da contratação pública, e sem prejuízo dos direitos dos titulares dos dados nos termos do artigo 79.º do RGPD. O Anexo V acrescenta as regras para os responsáveis pelo tratamento no Reino Unido e nos Estados Unidos.

13.3 Qualquer alteração ao presente Acordo deve ser feita por escrito; basta um e-mail. O Subcontratante publica o modelo em vigor em https://eco-heroes.org/trust/. Uma nova versão do modelo não altera um Acordo assinado sem o acordo do Responsável pelo tratamento. O administrador escolar do Responsável pelo tratamento pode aceitar o presente Acordo em linha; o Subcontratante regista quem o aceitou, quando, que versão e um hash com chave do endereço IP utilizado.

Assinaturas

Pelo Responsável pelo tratamento	Pelo Subcontratante — Eco Heroes International SL
Nome, cargo	Karim Zouhdi, fundador
Data, assinatura	Data, assinatura

Anexo I — Descrição do tratamento

A. Tratamento por conta do Responsável pelo tratamento (objeto do presente Acordo)

Anexo I.A — tratamento por conta do Responsável pelo tratamento

Elemento	Descrição
Objeto	Prestação do Serviço aos Utilizadores do Responsável pelo tratamento ao abrigo da Licença.
Natureza	Alojamento, armazenamento, apresentação e apagamento de dados; acompanhamento do progresso; quizzes de turma ao vivo; trabalhos; certificados; gestão de turmas; importação facultativa de listas de turma fornecidas pelo Responsável pelo tratamento (colar ou carregar CSV, CSV OneRoster 1.1/1.2, Google Classroom); acessos facultativos LTI 1.1 / LTI 1.3 a partir da plataforma de aprendizagem do Responsável pelo tratamento, com Names and Role Provisioning (importação de listas) e Assignment and Grade Services (devolução de pontuações); início de sessão facultativo dos professores com Google ou Microsoft escolhido pelo Responsável pelo tratamento; painel de turma da aplicação móvel Eco Heroes quando o Responsável pelo tratamento distribui um código de turma; questionários facultativos de estudos de impacto nas turmas inscritas pelo Responsável pelo tratamento; contas de coordenador, códigos de adesão de grupo e relatórios de progresso por grupo (CSV) para as licenças de empresas e hotéis; apoio. Nas licenças de empresa e de hotel, também: relatórios de atividade agregados para a organização (relatório da organização e totais, com qualquer número baseado em menos de 5 famílias oculto) e uma classificação por equipas opcional; o nome e o logótipo da organização nos certificados das crianças; início de sessão opcional do pessoal através do fornecedor de identidade do próprio Responsável (OpenID Connect).
Finalidade	Proporcionar educação para o desenvolvimento sustentável com base nos Objetivos de Desenvolvimento Sustentável das Nações Unidas, com o acompanhamento do progresso, os relatórios e a avaliação previstos na Licença. Nos estudos de impacto: a avaliação, pelo Responsável pelo tratamento, do seu próprio ensino (resultados de turma para os seus professores) e estatísticas agregadas e anonimizadas nos termos da cláusula 2.3. Nenhuma outra finalidade.
Categorias de titulares dos dados	Alunos (o jogo destina-se a idades dos 9 aos 17 anos em dois escalões, 9–12 e 13–17; as fichas de aula imprimíveis abrangem as faixas 6–10, 11–13 e 14–17 anos, e o Responsável pelo tratamento pode utilizar o Serviço com alunos mais novos segundo o seu critério); professores; administradores escolares; pais e representantes legais, apenas quando é utilizado o procedimento de consentimento; nas licenças de empresas e hotéis, os filhos dos trabalhadores ou dos hóspedes e os coordenadores da organização.

Elemento	Descrição
Dados pessoais — alunos (sítio web, numa turma)	Nome próprio ou alcunha introduzido pelo aluno ou pelo professor (2 a 24 caracteres; a partir de importações de listas, nome próprio e inicial, alargada no máximo às 3 primeiras letras do apelido apenas para distinguir dois alunos com o mesmo nome próprio — nunca o nome completo); escalão etário escolhido no jogo (9–12 ou 13–17); avatar de um conjunto fixo; língua; progresso (pontos, objetivos e missões concluídos, estrelas do quiz, número de perguntas respondidas e corretas por tema); trabalhos concluídos; data de adesão e da última atividade; um token de turma aleatório guardado no dispositivo do aluno para que o progresso possa ser gravado. Num quiz de turma ao vivo: a alcunha introduzida, as respostas, os tempos de resposta e a pontuação. Não são recolhidos: endereço de e-mail, apelido, fotografia, data de nascimento, morada, localização, identificadores do dispositivo ou de publicidade.
Dados pessoais — alunos (acessos LTI)	Um hash com chave do identificador de utilizador da plataforma (para associar um aluno a um lugar); o identificador de utilizador da plataforma no registo de acesso durante 90 dias, apenas quando a plataforma concedeu o serviço de classificações (necessário para a devolução de pontuações); nome próprio e inicial do apelido como alcunha; identificador e título do curso; funções; definições regionais; última pontuação enviada. Não são guardados nem o endereço de e-mail nem o nome completo; o Responsável pelo tratamento configura a sua plataforma para partilhar apenas o nome.
Dados pessoais — alunos (aplicação móvel, painel de turma)	Atividade (jogo diário jogado, data, língua, pontos, conclusão, duração; objetivos alcançados, distintivos) e um hash unidirecional de um identificador de instalação aleatório gerado pela aplicação. Os alunos aparecem ao professor sob um pseudónimo gerado. O painel não mostra nada para uma turma com menos de cinco alunos ativos.
Dados pessoais — alunos (estudo de impacto, quando o Responsável pelo tratamento inscreve uma turma)	Respostas ao questionário do estudo (escolhas, classificações e respostas curtas facultativas de texto livre), versão do questionário, língua, escalão etário, horas de início e de envio e indicadores de qualidade. Os endereços de e-mail e os números de telefone são retirados do texto livre na receção. As respostas que possam conter uma revelação relevante para a proteção de crianças são assinaladas ao contacto designado pelo Responsável pelo tratamento. As respostas são ligadas entre as fases do estudo por um hash unidirecional com chave do lugar do aluno na turma; não são recolhidos nome, endereço de e-mail nem data de nascimento. Para cada lugar, a oposição ou o consentimento escrito registado pelo Responsável pelo tratamento. Se não tiver sido designado um contacto para a proteção de crianças, os destinatários previstos na cláusula 4.4 ocupam o seu lugar.
Dados pessoais — professores e administradores escolares	Nome, endereço de e-mail profissional, escola, função (professor ou administrador escolar), língua; palavra-passe (hash bcrypt) ou identificador de início de sessão único; segredo da autenticação de dois fatores e códigos de recuperação com hash, se ativada (obrigatória para os administradores escolares); estado de verificação do e-mail; horas e número de inícios de sessão; sessões; turmas criadas; pré-visualizações de importações de listas (apenas nomes, mantidas na sessão durante 30 minutos); entradas do registo de auditoria das ações administrativas (com um hash com chave do endereço IP e o país da ligação como código de 2 letras fornecido pela rede de distribuição de conteúdos); correspondência de apoio.

Elemento	Descrição
Dados pessoais — professores (estudo de impacto)	Respostas ao questionário do professor e, para alunos dos 6 aos 8 anos, a ficha de observação da turma, ligadas por um hash unidirecional com chave da conta ou do código do professor; a inscrição da turma, o seu modo de consentimento e a sua afetação a um grupo do estudo.
Dados pessoais — pais e representantes legais	Apenas quando é utilizado o procedimento de consentimento parental do sítio web para um aluno abaixo da idade de consentimento digital: um hash unidirecional com chave do endereço de e-mail do pai ou da mãe (o próprio endereço é utilizado uma única vez para enviar a ligação de confirmação e não é guardado), a decisão e os respetivos carimbos temporais.
Dados pessoais — crianças e coordenadores (licenças de empresas e hotéis)	Filhos dos trabalhadores ou dos hóspedes do Responsável pelo tratamento: aderem a um grupo com o código de adesão do Responsável pelo tratamento e um nome de herói (alcunha) no seu próprio dispositivo ou num dispositivo da família, sem conta e sem endereço de e-mail. O Serviço guarda os mesmos dados que para os alunos de uma turma: nome de herói, escalão etário, avatar, língua, progresso e resultados dos quizzes. Coordenadores: nome, endereço de e-mail profissional, hash da palavra-passe ou identificador de início de sessão, definições de autenticação de dois fatores e os grupos que abrem. O coordenador vê os objetivos concluídos e os resultados dos quizzes por grupo e pode exportá-los em CSV. Para o relatório da organização, o Serviço regista também, para cada perfil de herói destes grupos, os dias com atividade e o dia em que cada objetivo ou missão foi concluído pela primeira vez (com precisão ao dia; as turmas das escolas não são registadas assim). Os relatórios contêm apenas dados agregados: nenhum nome, alcunha, identificador ou linha por criança; qualquer número baseado em 1 a 4 famílias fica oculto (k = 5), e um segundo número fica oculto quando um só permitiria deduzi-lo. Os nomes das equipas são escolhidos pelo administrador do Responsável e não podem identificar pessoas. Quando o Responsável ativa o início de sessão da empresa, os nomes e e-mails do pessoal vêm do fornecedor de identidade do próprio Responsável (âmbitos openid, email e profile); esse fornecedor de identidade é um sistema e um subcontratante do próprio Responsável, não um Subcontratante ulterior, e o seu identificador de sujeito é guardado apenas como hash com chave. Marca partilhada: o nome visível e o logótipo da organização, fornecidos pelo Responsável. A página pública do distintivo que um pai, uma mãe ou um tutor pode partilhar no LinkedIn não contém dados pessoais (um número de objetivos, o nome da organização se o Responsável o ativou, e uma língua, tudo retirado da sua ligação); é o adulto que inicia a partilha, e o Subcontratante não envia nada ao LinkedIn.
Categorias especiais (artigo 9.º do RGPD)	Nenhuma é pedida ou necessária. Ver a cláusula 4.2.
Frequência	Contínua, durante a vigência da Licença.

B. Tratamentos de que a Eco Heroes é responsável de forma independente (fora do presente Acordo)

Enumerados para que o Responsável pelo tratamento veja onde termina o presente Acordo. Regem-se pela Política de Privacidade (v4.3) e pelo Aviso de Privacidade para Crianças (v2.2) do Subcontratante, e não pelo presente Acordo:

- **As contas de professor enquanto tais:** início de sessão, segurança, autenticação de dois fatores e recursos gratuitos para professores. O Subcontratante é responsável pela própria conta e apaga-a nos

termos da cláusula 10.4; a atividade da conta para o Responsável pelo tratamento constitui Dados do Responsável.

- **Contas gratuitas de professor:** professores não associados a uma licença que utilizam os recursos gratuitos para professores com um endereço de e-mail verificado.
- **Subscrições familiares** no sítio web, contratadas por um pai, mãe ou representante legal: o endereço de e-mail (guardado parcialmente ocultado), as referências de pagamento e de subscrição da Stripe e um código de acesso pessoal (guardado como hash com chave). Os dados do cartão nunca chegam ao Subcontratante. Um código familiar utilizado na escola não transporta dados da escola.
- **Contas da aplicação** (início de sessão dos pais com Google ou Apple; subscrições através do Google Play ou da Apple; estado da subscrição através da RevenueCat).
- **Visitantes do sítio web** nas páginas públicas para adultos (Google Analytics 4 após consentimento; o formulário de contacto através da Formspree; os pedidos de orçamento e as candidaturas a embaixador através do servidor próprio do Subcontratante; os e-mails Dinner Questions através da Brevo).
- **Tabela de classificação pública do quiz** (facultativa: uma alcunha escolhida de uma lista gerada, a pontuação e um hash com chave do endereço IP; conservados durante 30 dias).
- **Inquéritos do programa** que o Subcontratante realiza fora de uma turma, com o consentimento de um pai ou mãe quando a lei o exija.
- **Serviços distintos:** a Eco Heroes Academy (learn.eco-heroes.org) e a avaliação VSME (assessment.eco-heroes.org) têm termos e informações de privacidade próprios.

C. Calendário de conservação (tal como aplicado no Serviço)

Anexo I.C — calendário de conservação

Dados	Conservação	Mecanismo
Dados de alunos e de crianças em grupos de empresas e hotéis (alcunha, escalão etário, avatar, progresso, trabalhos, atividade de turma na aplicação, associação de lugares LTI)	Durante a Licença: até que um professor ou administrador apague o aluno ou a turma. Após o termo da Licença: apagamento 90 dias após a data de termo, salvo renovação da Licença. A pedido escrito do Responsável pelo tratamento: apagamento no prazo de 30 dias; os administradores da escola recebem um aviso por e-mail 30 e 7 dias antes do apagamento	Ação do professor ou do administrador no Serviço; apagamento automático no fim da licença; o Subcontratante a pedido escrito
Datas de atividade dos perfis de herói em grupos de empresa e de hotel (relatório da organização)	Guardadas com o perfil de herói e apagadas com ele, segundo a regra acima	Eliminação com o perfil
Definições da organização: nomes das equipas e equipa de cada grupo, ativação da classificação por equipas, nome e logótipo da marca partilhada, configuração do início de sessão da empresa	Durante a vigência da Licença; apagadas a pedido do Responsável	Subcontratante, a pedido

Dados	Conservação	Mecanismo
Início de sessão da empresa: registos do processo de início de sessão; ligações de identidade fixadas (hash com chave do sujeito do fornecedor de identidade)	Registos do processo: apagados ao serem usados ou após 10 minutos. Ligações de identidade: até a conta ser apagada ou a configuração de início de sessão do Responsável ser removida ou reposta	Limpeza automática; ação de um administrador
Quizzes de turma ao vivo (alcunhas, respostas, tempos, pontuações)	30 dias após a criação da sessão do quiz	Limpeza diária automática
Pré-visualizações de importações de listas (OneRoster)	30 minutos, apenas na sessão de servidor do professor	Expiração da sessão
Token de acesso do Google Classroom (importação de listas)	Apenas durante a importação, na sessão do professor; nunca escrito na base de dados	Expiração da sessão
Registos de acesso LTI	Acessos de professores, e acessos de alunos sem serviço de classificações: 2 horas. Acessos de alunos com serviço de classificações: 90 dias	Limpeza automática durante a atividade LTI
Estado de início de sessão LTI, tokens de passagem, tokens de ligação profunda, nonces, tokens de importação de listas	10 minutos / 10 minutos / 60 minutos / 15 minutos / 2 horas	Limpeza automática; utilização única
Contas de professores, de coordenadores e de administradores escolares	12 meses após o termo da última licença associada à conta; contas gratuitas após 12 meses sem início de sessão; e-mail de aviso 30 dias antes do apagamento. Registos não verificados: apagados 7 dias depois de expirar a última ligação de confirmação	Limpeza automática de contas
Sessões e «lembrar-me»	Sessão de servidor durante a duração configurada, renovada no início de sessão e a cada 30 minutos; todas as sessões terminam com a mudança de palavra-passe ou quando um administrador retira o acesso. Cookie «lembrar-me»: 180 dias (assinado com HMAC)	Código
Registos de limitação de pedidos (tentativas de início de sessão e outros limites)	30 dias	Limpeza diária automática
Registo de auditoria de segurança (ações administrativas, ativações de códigos e inícios de sessão; hash com chave do IP, país da ligação como código de 2 letras)	12 meses	Limpeza diária automática
Hashes de IP antiabuso nas respostas a inquéritos e nos pedidos de consentimento	30 dias (a própria resposta segue o seu próprio prazo)	Limpeza diária automática

Dados	Conservação	Mecanismo
Pedidos de consentimento parental	Sem resposta ou expirados: 30 dias. Recusas: 12 meses. Consentimento dado: enquanto for invocado; apagado juntamente com os dados se o consentimento for retirado	Limpeza diária automática; função de apagamento
Respostas a estudos de impacto (alunos, professores, fichas de observação) e marcas de oposição ou de consentimento	24 meses após o encerramento da última fase do estudo; mais cedo mediante instrução escrita do Responsável pelo tratamento. As marcas de oposição e de consentimento são apagadas juntamente com a inscrição da turma	Limpeza diária automática; o Subcontratante a pedido escrito
Alertas de proteção de crianças (respostas a estudos de impacto que podem conter uma revelação, com o lugar e a alcunha a que pertencem)	O texto da resposta é apagado 30 dias depois de o alerta ser marcado como tratado; o registo do alerta é apagado 12 meses depois de tratado	Limpeza diária automática
Respostas a inquéritos do programa	24 meses, ou até à retirada do consentimento	Limpeza diária automática; função de apagamento
Entradas da tabela de classificação pública do quiz (fora do presente Acordo, enumeradas para que fique completo)	30 dias	Limpeza diária automática
Registos da aceitação do presente Acordo pelo Responsável pelo tratamento (quem o aceitou, quando, que versão, hash com chave do endereço IP; conservados pelo Subcontratante enquanto responsável pelo tratamento, cláusula 13.3)	Enquanto a Licença durar e 6 anos após o seu fim	Registos do Subcontratante
Registos da aceitação no pagamento, de cancelamento e de resolução dos planos familiares (fora do presente Acordo, enumerados para que fique completo)	6 anos, com os registos contabilísticos (Código Comercial espanhol, artigo 30.º)	Registos contabilísticos
Contador da taxa de participação derivado de uma pessoa	2 dias	Limpeza diária automática
Telemetria (relatórios de violações de CSP e de erros JavaScript)	Nenhum identificador guardado (user agent truncado); contadores de limitação repostos a cada minuto; registo limitado a 5 MB	Código
Correspondência de apoio (e-mail)	Até o pedido ser tratado, e no máximo 12 meses após a última mensagem	Procedimento da caixa de correio do Subcontratante

Dados	Conservação	Mecanismo
Cópias de segurança cifradas	Cópias cifradas conservadas de forma rotativa; os dados apagados saem de todas as cópias de segurança no prazo de 14 dias	Automático
Réplica de reserva da base de dados	Contínua; acompanha cada apagamento	Replicação
Registos técnicos do servidor web (endereço IP, endereço pedido)	Até 90 dias	Configuração do servidor
Faturas e registos de pagamento	6 anos (Código Comercial espanhol, artigo 30.º); identificam as pessoas de contacto do Responsável pelo tratamento, nunca os alunos	Registos contabilísticos

Anexo II — Medidas técnicas e organizativas (artigo 32.º do RGPD)

As medidas em vigor à data do presente Acordo. São revistas em cada versão, e o resumo em vigor está publicado em https://eco-heroes.org/trust/#security. O Subcontratante pode atualizar as medidas, desde que o nível global de segurança não diminua.

1. Cifragem em trânsito

- TLS 1.2 ou superior em todas as ligações; HTTP Strict Transport Security com max-age de dois anos, includeSubDomains e preload; renovação automática dos certificados; certificados de origem entre a rede de distribuição de conteúdos e os servidores.
- Os servidores de aplicações só se ligam à base de dados através de TLS 1.2/1.3, com verificação do certificado face a uma autoridade de certificação fixada; a base de dados recusa ligações não cifradas (require_secure_transport). As contas da base de dados estão limitadas aos anfitriões de aplicações e de reserva.
- As cópias de segurança são cifradas (AES-256-CBC, PBKDF2 com 200 000 iterações) antes de saírem do servidor e só circulam por ligações cifradas. Não são escritos arquivos não cifrados.

2. Proteção no navegador

- Content-Security-Policy: os scripts inline só são executados se aprovados por um hash SHA-256 por script, ou por um nonce por pedido em algumas páginas dinâmicas (sem unsafe-inline para scripts — os estilos inline continuam permitidos; object-src 'none', base-uri 'self', frame-ancestors 'none' exceto nas páginas LTI, que só as plataformas de aprendizagem registadas podem incorporar). Os relatórios de violação são recolhidos, com limitação de pedidos. As páginas para crianças não carregam scripts de terceiros. Nas páginas para adultos, os únicos scripts de terceiros são o Google Analytics, após consentimento, e a verificação Cloudflare Turnstile nos formulários de início de sessão e de registo.
- Os tipos de letra web estão alojados no servidor próprio do Subcontratante. Não é enviado qualquer pedido ao Google Fonts nem a outro fornecedor de tipos de letra.
- Cabeçalhos de segurança: X-Content-Type-Options: nosniff, X-Frame-Options: DENY, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy e Cross-Origin-Resource-Policy same-origin. Os cabeçalhos de versão do servidor e do PHP são removidos. HTTP TRACE e TRACK são recusados.
- Cookies: o cookie de sessão é Secure, HttpOnly e SameSite=Strict, em modo de sessão estrito; o identificador de sessão muda no início de sessão, na ativação de um código e a cada 30 minutos. O cookie «lembrar-me» é assinado com HMAC com uma chave do lado do servidor. O cookie de estado LTI está limitado a /lti/ e particionado.
- O service worker dos jogos nunca guarda em cache respostas marcadas como no-store ou private nem qualquer caminho reservado a membros, pelo que nenhum conteúdo reservado fica na cache de um dispositivo partilhado após terminar a sessão.
- As respostas que contêm dados pessoais ou conteúdo reservado a membros são enviadas com Cache-Control: private, no-store, e a rede de distribuição de conteúdos nunca as guarda em cache.

3. Controlo de acessos e autenticação

- Contas de professor nominativas: um código de escola é utilizado uma única vez, para a inscrição. Cria uma conta nominativa com um endereço de e-mail verificado, ou associa a escola à conta que o professor já tem. Depois, o professor inicia sessão com o seu próprio endereço de e-mail e palavra-passe, ou por início de sessão único. Um dispositivo em que apenas foi introduzido um código de escola

pode jogar, mas não tem ferramentas de professor. Um código de administração cria apenas a primeira conta de administração da escola e fica esgotado quando essa conta é confirmada; os professores juntam-se depois com um código de pessoal que um administrador da escola cria no Serviço, mostrado uma única vez, guardado apenas como hash com chave e substituível a qualquer momento.

- As palavras-passe dos professores são transformadas com bcrypte comparadas em tempo constante. O endereço de e-mail tem de ser verificado antes do primeiro início de sessão. A mudança de palavra-passe termina todas as sessões. Um administrador escolar pode retirar imediatamente o acesso a um professor.
- A autenticação de dois fatores (TOTP, com códigos de recuperação com hash) é obrigatória para os administradores escolares e para os superadministradores do Subcontratante, e qualquer professor ou coordenador de uma licença de empresa ou de hotel a pode ativar. O código QR de registo é gerado no servidor, pelo que o segredo nunca sai dele. O segundo fator é verificado antes de ser criada qualquer sessão, e os administradores escolares têm de o utilizar sempre que haja dados de alunos visíveis. O contacto para a proteção de crianças também tem de o utilizar para ler os alertas de proteção. Após 10 códigos errados em 24 horas, o segundo fator da conta fica bloqueado durante 15 minutos e o titular da conta é avisado por e-mail.
- Os códigos de acesso só são guardados como hashes com chave num ficheiro fora da raiz web; a chave é guardada fora da raiz web. Os códigos de registo e de licença são guardados da mesma forma; um código é mostrado uma única vez, quando é criado.
- Limitação de pedidos no início de sessão (por endereço IP e por par e-mail/IP, com um teto global), no registo, no resgate de códigos, na adesão a turmas, na adesão a quizzes ao vivo, na sincronização do progresso, no formulário de orçamento, nos inícios de sessão LTI, nos pontos de telemetria e nas consultas de retorno da Stripe. Tokens CSRF em todos os formulários que alteram dados. Proteção contra redirecionamentos abertos em todos os parâmetros next=.
- Direitos de acesso verificados no servidor: os recursos reservados a membros (vídeos das missões, bancos de perguntas do quiz, livros, conteúdos LTI) só são servidos depois de o servidor verificar uma sessão de código válida, um código memorizado assinado ou uma conta com sessão iniciada. Nada do que o navegador escreve por si próprio concede acesso.
- Isolamento por função e por escola: cada professor vê apenas as suas próprias turmas; os administradores escolares veem todas as turmas da sua própria escola e nada das outras escolas; os professores que entram por LTI veem apenas as turmas do curso a partir do qual acederam; o acesso de superadministrador está limitado ao pessoal do Subcontratante nominalmente identificado.
- Todas as consultas à base de dados utilizam instruções preparadas; sem exec, eval nem unserialize; os caminhos de ficheiros só são construídos a partir de elementos de uma lista autorizada; os carregamentos (ficheiros CSV/ZIP de listas de turma, imagens de inquéritos) têm limite de tamanho, tipo verificado e são guardados fora da raiz web; a apresentação de erros PHP está desativada.
- Início de sessão único opcional para o pessoal de empresas e hotéis através de OpenID Connect (Authorization Code com PKCE; tokens de identidade assinados e verificados quanto ao emissor, audiência, validade e nonce). Os segredos de cliente são cifrados em repouso. As contas só são associadas dentro dos domínios de e-mail autorizados do Responsável e nunca são ligadas a uma conta de outra organização.

4. Minimização de dados e dados de crianças

- Não são recolhidos endereços de e-mail, apelidos, fotografias, datas de nascimento, moradas, localizações nem identificadores do dispositivo ou de publicidade dos alunos. As importações de listas

mantêm o nome próprio e no máximo as 3 primeiras letras do apelido. Os alunos que entram por LTI são guardados com um hash com chave do identificador de utilizador da plataforma, com nome próprio e inicial; o Responsável pelo tratamento configura a sua plataforma para partilhar apenas o nome.

- Os endereços IP só são guardados como hashes com chave (prefixo). Quem detém a chave poderia voltar a associá-los; são, por isso, pseudonimizados e não anónimos. Quando acompanham um conteúdo, são apagados ao fim de 30 dias.
- As páginas para crianças (/game, /games, /trivia, /library, /sdg, /wordle, /missions, /books e as suas versões linguísticas) não carregam análises nem mostram um banner de consentimento. Nas restantes páginas, as análises só carregam após consentimento explícito.
- Os vídeos das missões reservados a membros são alojados pelo Subcontratante e servidos após verificação dos direitos de acesso. Onde ainda existe um leitor do YouTube (jogo livre), utiliza youtube-nocookie.com e só carrega quando o utilizador toca em reproduzir.
- A publicação na tabela de classificação pública do quiz é facultativa depois de cada jogo, com uma alcunha gerada (um adjetivo e um animal; sem texto livre nem nome de escola). A tabela pública mostra a alcunha e a pontuação dos 10 melhores dos últimos 30 dias, e as entradas são apagadas ao fim de 30 dias. Cada linha pública tem uma ligação de denúncia; uma linha denunciada três vezes fica oculta até ser analisada. As tabelas de turma só são visíveis para o professor dessa turma e para os administradores da escola, que podem retirar linhas.
- As respostas de texto livre são filtradas automaticamente quando são enviadas: os endereços de e-mail e os números de telefone são retirados, e as respostas que correspondem a uma pequena lista de palavras que podem indicar que uma criança está em risco são retiradas dos dados do estudo e transmitidas apenas ao contacto para a proteção de crianças designado pela escola. Os nomes não são retirados automaticamente; os investigadores que leem as respostas assinalam os possíveis nomes e nunca os incluem em relatórios. Uma possível revelação é transmitida ao contacto designado pela escola no prazo de um dia letivo. Se não tiver sido designado um contacto para a proteção de crianças, os destinatários previstos na cláusula 4.4 ocupam o seu lugar.
- Os endereços de e-mail dos pais no procedimento de consentimento nunca são guardados em claro; apenas é conservado um hash com chave.
- Os relatórios da organização são agregados: um número baseado em menos de 5 famílias fica oculto no próprio cálculo, pelo que nem o ecrã nem o CSV o podem mostrar. Só os administradores da organização, com início de sessão em dois passos, os podem abrir; cada consulta e cada exportação têm um limite de frequência e ficam registadas.

5. Disponibilidade, cópias de segurança e recuperação

- As operações seguintes são executadas automaticamente. Uma monitorização independente (UptimeRobot, 11 sondas, a cada 5 minutos) alerta o Subcontratante em caso de falha.
- Todas as noites, uma cópia de segurança cifrada da base de dados e da aplicação; uma cópia é guardada num centro de dados separado noutro país da UE. Todos os meses é testada automaticamente uma reposição.
- Uma cópia de segurança antes de cada versão, com um procedimento de reversão testado; a versão de produção anterior é conservada.
- Um servidor de reserva mantém uma cópia da aplicação e uma réplica ativa da base de dados. Se o servidor web principal falhar, um balanceamento de carga com verificações de estado desvia o tráfego automaticamente; se o servidor da base de dados falhar, a réplica é promovida através de um procedimento automatizado e ensaiado. Ambos foram testados em outubro de 2026.

- Uma verificação horária da infraestrutura (estado e atraso da réplica, expiração dos certificados, espaço em disco, atualizações de segurança pendentes, intervalos de endereços da rede de distribuição de conteúdos). As atualizações de segurança do sistema operativo são instaladas automaticamente. Proteção contra ataques DDoS e bots na periferia da rede.
- O ambiente de pré-produção está separado da produção (utilizador Unix distinto, pool PHP com open_basedir, instância de base de dados distinta, segredos retirados).

6. Registo e monitorização

- Os eventos de segurança (inícios de sessão falhados, resgates de códigos, ações administrativas, relatórios de violação de CSP, apagamentos e limpezas de conservação) são registados com hashes com chave dos endereços IP. O registo de auditoria de segurança é conservado durante 12 meses e os registos de limitação de pedidos durante 30 dias (Anexo I, secção C).
- O estado do serviço em tempo real e cada interrupção são publicados na página pública de estado.

7. Medidas organizativas

- O acesso aos sistemas de produção está limitado a pessoas nominalmente identificadas. Todas as contas administrativas (alojamento, servidores da base de dados e das cópias de segurança, rede de distribuição de conteúdos e DNS, repositório de código-fonte, monitorização, correio eletrónico) utilizam autenticação de dois fatores. O acesso aos servidores faz-se com chaves SSH. As firewalls limitam o acesso à base de dados e ao servidor de reserva aos anfitriões próprios do Subcontratante e aos intervalos de endereços da rede de distribuição de conteúdos.
- As alterações são testadas automaticamente (integração contínua; uma versão é recusada se o código não passou nos testes), passam primeiro pela pré-produção e são verificadas em produção após cada versão (47 verificações em direto). É realizada e documentada uma revisão estática de segurança da aplicação (a mais recente: 16 de outubro de 2026).
- Teste de intrusão, outubro de 2026: um teste estruturado de caixa branca e caixa cinzenta da plataforma (autenticação, sessões, controlo de acesso entre escolas, pagamentos, exposição de ficheiros e dados, limitação de tentativas e cache na periferia da rede), realizado pela própria equipa de testes do Subcontratante. Todas as vulnerabilidades críticas, altas e médias encontradas foram corrigidas e testadas novamente antes da publicação. Está previsto um teste de intrusão externo, a cargo de uma empresa independente.
- Está publicado um canal de comunicação de vulnerabilidades em /.well-known/security.txt. As comunicações são confirmadas no prazo de 5 dias úteis e os problemas críticos são corrigidos antes de qualquer outro trabalho.
- Um procedimento escrito de gestão de incidentes descreve a forma como o Subcontratante deteta, contém e regista uma violação de dados pessoais e como cumpre o prazo de notificação de 48 horas da cláusula 9.
- O Subcontratante conserva um registo dos tratamentos que realiza por conta de responsáveis pelo tratamento (artigo 30.º, n.º 2, do RGPD) e uma avaliação da transferência para cada Subcontratante ulterior fora do EEE.
- Os prazos de conservação estão definidos no código que os aplica, pelo que o prazo publicado e o prazo aplicado não podem divergir.
- Os segredos (chave restrita da Stripe, credenciais de início de sessão único, chaves de hash) são guardados fora da raiz web e nunca são incluídos no repositório de código-fonte.

Anexo III — Subcontratantes ulteriores e serviços de terceiros

O Trust Centre (https://eco-heroes.org/trust/#subprocessors) mostra as mesmas duas listas.

Parte A — Subcontratantes ulteriores que tratam Dados do Responsável

Anexo III.A — subcontratantes ulteriores autorizados

Subcontratante ulterior	O que faz	Onde	Garantia para a transferência
Internet Girona, em infraestrutura OVHcloud	Alojamento web	França (UE)	Na UE; termos normais de tratamento de dados do fornecedor
Hetzner Online GmbH, Gunzenhausen, Alemanha	Alojamento da base de dados, servidor de reserva e cópias de segurança cifradas	Alemanha e Finlândia (UE)	Na UE; termos normais de tratamento de dados da Hetzner
Cloudflare, Inc., São Francisco, EUA	Distribuição de conteúdos, TLS, proteção contra ataques e bots, verificação Turnstile nos formulários de início de sessão e de registo, e comutação automática em caso de falha	Rede periférica mundial; servidores de origem na UE	Termos normais de tratamento de dados da Cloudflare com as cláusulas contratuais-tipo (2021/914); Quadro de Privacidade de Dados UE-EUA quando a Cloudflare consta da lista
Proton AG, Genebra, Suíça	Alojamento do correio eletrónico info@ e security@eco-heroes.org: correspondência de apoio e de proteção de dados com o pessoal do Responsável pelo tratamento	Suíça	Decisão de adequação da Comissão Europeia para a Suíça; termos normais de tratamento de dados da Proton
Google (Google Ireland Ltd / Google LLC) — apenas início de sessão e importação do Classroom	Apenas se o Responsável pelo tratamento os ativar: início de sessão dos professores (nome, endereço de e-mail, identificador; nenhum dado de alunos); importação de listas do Google Classroom (nome próprio e apelido lidos uma vez e guardados como nome próprio e inicial; o token de acesso fica na sessão do professor)	UE / EUA	Termos Google próprios do Responsável pelo tratamento; termos normais de tratamento de dados da Google com as cláusulas contratuais-tipo; Quadro de Privacidade de Dados UE-EUA quando consta da lista
Microsoft (Microsoft Ireland Operations Ltd) — apenas início de sessão	Apenas se o Responsável pelo tratamento o ativar: início de sessão dos professores (apenas identidade; nenhum dado de alunos)	UE / EUA	Termos Microsoft próprios do Responsável pelo tratamento; Microsoft Products and Services DPA com as cláusulas contratuais-tipo; Quadro de Privacidade de Dados UE-EUA quando consta da lista

Subcontratante ulterior	O que faz	Onde	Garantia para a transferência
Google (YouTube, youtube-nocookie.com)	Reprodução de vídeos educativos selecionados onde ainda se utiliza um leitor do YouTube: modo de privacidade melhorada, carregado apenas quando o utilizador toca em reproduzir	UE / EUA	Termos da Google; Quadro de Privacidade de Dados UE-EUA quando consta da lista
Moodle Pty Ltd (MoodleCloud), Austrália Ocidental	Apenas se o Responsável pelo tratamento utilizar o sítio de cursos Eco Heroes eco-heroes.moodlecloud.com em vez da sua própria plataforma de aprendizagem: contas de curso nesse sítio e o progresso que os jogos lá registam	Alojamento MoodleCloud na Amazon Web Services	Acordo de tratamento de dados da MoodleCloud com as cláusulas contratuais-tipo (2021/914) para qualquer transferência para fora do EEE

Parte B — Serviços de terceiros que não tratam Dados do Responsável

Enumerados por transparência. Quando estão em causa dados pessoais, aplica-se a Política de Privacidade do Subcontratante. O servidor de correio próprio do Subcontratante envia os e-mails de conta, de verificação e de serviço; não é um terceiro.

Anexo III.B — serviços de terceiros fora do presente Acordo

Serviço	O que faz	Onde	Por que razão está fora do presente Acordo
Stripe	Pagamentos com cartão das subscrições familiares no sítio web; o Subcontratante consulta o estado do pagamento e da subscrição	UE / EUA; termos de tratamento de dados da Stripe com as cláusulas contratuais-tipo; Quadro de Privacidade de Dados UE-EUA	Os subscritores familiares são clientes próprios do Subcontratante; não são enviados dados da escola à Stripe
Google Analytics 4	Estatísticas de visitas nas páginas públicas para adultos, apenas após consentimento; nunca nas páginas para crianças nem na área de professores	UE / EUA; termos de tratamento de dados da Google com as cláusulas contratuais-tipo; Quadro de Privacidade de Dados UE-EUA	Não são enviados Dados do Responsável; o Subcontratante é responsável pelas suas próprias estatísticas web
Formspree	Encaminha as mensagens enviadas através do formulário de contacto geral	EUA; termos normais de tratamento de dados do fornecedor (cláusulas contratuais-tipo; Quadro de Privacidade de Dados UE-EUA quando consta da lista)	As mensagens são correspondência própria do Subcontratante; não utilizado pelo Serviço
Brevo	E-mails Dinner Questions para famílias (mediante inscrição; apenas endereço de e-mail)	UE	Boletim informativo para famílias; não utilizado pelo Serviço
RevenueCat	Estado da subscrição na aplicação (apenas identificador da conta e histórico de compras)	EUA; cláusulas contratuais-tipo	Contas familiares da aplicação; nenhum dado da escola

Serviço	O que faz	Onde	Por que razão está fora do presente Acordo
Google Play / Apple App Store	Pagamentos das subscrições na aplicação, cobrados pela loja	UE / EUA	As lojas vendem a subscrição na qualidade de responsáveis independentes pelo tratamento
Google / Apple (início de sessão na app)	Início de sessão facultativo dos pais na aplicação (endereço de e-mail e identificador de início de sessão)	UE / EUA; Quadro de Privacidade de Dados UE-EUA, cláusulas contratuais-tipo	Contas familiares da aplicação; nenhum dado da escola
UptimeRobot	Verifica se as páginas públicas e o ponto de estado respondem	UE / EUA	Não trata dados pessoais

Anexo IV — Dados de crianças

O presente anexo completa os Anexos I e II para os alunos com menos de 18 anos.

1. **Idade de consentimento digital.** Quando a lei aplicável ao Responsável pelo tratamento exija consentimento para serviços da sociedade da informação oferecidos diretamente a crianças (artigo 8.º do RGPD), o Responsável pelo tratamento obtém-no e regista-o. Essa idade é de 14 anos em Espanha (artigo 7.º da LOPDGDD), entre 13 e 16 anos nos outros Estados-Membros da UE e de 13 anos no Reino Unido; para as escolas nos Estados Unidos, ver o Anexo V. Quando o Responsável pelo tratamento se baseie noutro fundamento jurídico para a utilização escolar, por exemplo uma missão de interesse público, não é necessário consentimento e o Responsável pelo tratamento informa os alunos e os pais. O Serviço não verifica a idade. Os seus dois escalões etários (9–12 e 13–17) apenas selecionam o conteúdo e a versão dos vídeos.
2. **Procedimento de consentimento parental no sítio web.** Quando uma funcionalidade do sítio web exija o consentimento de um pai ou mãe para uma criança abaixo da idade de consentimento digital, o Serviço não guarda nada até o pai ou mãe confirmar através de uma ligação de utilização única enviada por e-mail. Só são guardados um hash com chave do endereço de e-mail do pai ou mãe, a decisão e os carimbos temporais. Os pedidos sem resposta são apagados ao fim de 30 dias e as recusas ao fim de 12 meses. A retirada do consentimento apaga os dados recolhidos com base nele.
3. **Plano familiar.** Um pai, mãe ou representante legal contrata a subscrição familiar e é cliente do Subcontratante. No sítio web, o pagamento pede ao comprador que confirme ser maior de idade; na aplicação, os passos de início de sessão e de compra estão atrás de uma verificação para adultos (uma pergunta de aritmética a escrever). Nenhuma delas é uma verificação de identidade ou de idade. As crianças não abrem contas no sítio web. Uma criança pode utilizar um código familiar sob a responsabilidade do pai ou mãe; não lhe estão associados dados de escola.
4. **Sem definição de perfis nem publicidade.** O Subcontratante não mostra publicidade e não utiliza identificadores nem SDK de publicidade. Não cria perfis de alunos para além do acompanhamento do progresso que os professores do Responsável pelo tratamento veem, não toma decisões automatizadas que produzam efeitos jurídicos ou efeitos igualmente significativos e nunca vende nem partilha dados de alunos para publicidade.
5. **Sem análises nas páginas para crianças.** As páginas para crianças (o jogo de aventura, a zona de jogos, o quiz, a biblioteca, as páginas dos objetivos, o Wordle, as missões e os livros, nas 13 línguas) não carregam análises, rastreadores nem banner de consentimento. Utilizam apenas o armazenamento do navegador estritamente necessário (língua, progresso no dispositivo, sessão).
6. **Estudos de impacto.** Quando o Responsável pelo tratamento inscreve turmas num estudo de impacto, os alunos respondem na aula no âmbito da avaliação que o Responsável pelo tratamento faz do seu próprio ensino. O Responsável pelo tratamento informa os pais com antecedência e dá-lhes a possibilidade de se oporem, ou recolhe um consentimento escrito quando a sua lei ou as suas regras o exijam; o Serviço suporta ambos e exclui os lugares em causa. Os alunos podem saltar qualquer pergunta e são disso informados no primeiro ecrã. Os professores só veem resultados de turma, e apenas quando pelo menos 10 alunos responderam antes e depois; nenhum utilizador da escola vê as respostas individuais de um aluno. Uma resposta de texto livre que possa conter uma revelação relevante para a proteção de crianças é encaminhada para o contacto designado pelo Responsável pelo tratamento, que decide o que fazer. O Subcontratante utiliza apenas resultados agregados e anonimizados nos termos da cláusula 2.3, nunca texto livre. Uma possível revelação é transmitida ao contacto designado no prazo de

um dia letivo, e só esse contacto a vê. Se não tiver sido designado um contacto para a proteção de crianças, os destinatários previstos na cláusula 4.4 ocupam o seu lugar.

7. **Sem funcionalidades de comunicação.** O Serviço não tem chat, mensagens nem perfis públicos de alunos. A tabela de classificação pública do quiz é facultativa, utiliza apenas alcunhas escolhidas de uma lista gerada, não mostra nomes de escolas, conserva as entradas durante 30 dias e tem uma ligação de denúncia em cada entrada. As tabelas de turma só são visíveis para o professor da turma e para os administradores da escola, e uma entrada pública denunciada três vezes fica oculta até ser analisada.
8. **Risco residual comunicado ao Responsável pelo tratamento.** Um colega que conheça um código de turma e a alcunha de um aluno pode abrir o progresso desse aluno noutro dispositivo. Os professores podem ver, mudar o nome ou retirar alunos a qualquer momento e podem renovar o código de turma. O Responsável pelo tratamento tem isso em conta na sua própria avaliação e na forma como distribui os códigos de turma.
9. **Direitos dos pais e dos alunos.** Os pais e os alunos exercem os seus direitos junto do Responsável pelo tratamento. Os professores do Responsável pelo tratamento podem consultar, exportar, mudar o nome, repor e apagar diretamente os dados de um aluno. O Subcontratante encaminha para o Responsável pelo tratamento qualquer pedido que receba (cláusula 8.2).
10. **Informação para as crianças.** O Subcontratante publica um Aviso de Privacidade para Crianças com uma parte escrita para crianças (Parte A) e uma parte para pais e escolas (Parte B) em https://eco-heroes.org/legal/children/. O Responsável pelo tratamento pode reproduzi-lo na sua própria informação a alunos e pais.

Anexo V — Responsáveis pelo tratamento no Reino Unido e nos Estados Unidos

1. **Reino Unido.** Quando o Responsável pelo tratamento estiver estabelecido no Reino Unido, as referências do presente Acordo ao RGPD entendem-se feitas ao UK GDPR e ao Data Protection Act 2018, e a autoridade de controlo competente é o Information Commissioner's Office (ICO). Os Dados do Responsável são transferidos do Reino Unido para o EEE ao abrigo dos regulamentos de adequação do Reino Unido relativos ao EEE. As transferências ulteriores para os Estados Unidos baseiam-se na extensão britânica do Quadro de Privacidade de Dados UE-EUA quando o fornecedor está certificado, ou no UK International Data Transfer Addendum às cláusulas contratuais-tipo. O Subcontratante concebe o Serviço tendo em conta o Age Appropriate Design Code do ICO; o seu resumo de conformidade consta da secção 11 da Política de Privacidade.
2. **Estados Unidos — FERPA.** Quando o Responsável pelo tratamento for uma escola ou um distrito escolar dos Estados Unidos sujeito ao Family Educational Rights and Privacy Act, o Subcontratante atua como «school official» com um interesse educativo legítimo na aceção de 34 CFR 99.31(a)(1)(i)(B). O Subcontratante está sob o controlo direto do Responsável pelo tratamento no que respeita à utilização e manutenção dos registos escolares, utiliza-os apenas para as finalidades da Licença e não os divulga a ninguém, exceto aos Subcontratantes ulteriores nos termos da cláusula 6 ou quando a lei o exija.
3. **Estados Unidos — COPPA.** Para alunos com menos de 13 anos, o Responsável pelo tratamento pode consentir, em nome dos pais, na recolha dos dados descritos no Anexo I, como permitem as orientações da Federal Trade Commission, uma vez que os dados são utilizados apenas para as finalidades educativas do Responsável pelo tratamento e para nenhuma outra finalidade comercial. O Responsável pelo tratamento mantém os pais informados e encaminha os seus pedidos para consultar ou apagar os dados do seu filho; o Subcontratante dá-lhes seguimento nos termos da cláusula 8.

4. **Estados Unidos — apagamento e notificação.** Ao apagamento no termo da Licença aplica-se a cláusula 10. Quando uma lei estadual sobre a privacidade dos alunos fixe um prazo mais curto para a notificação de violações ou para o apagamento, o Subcontratante cumpre-o logo que o Responsável pelo tratamento lhe indique qual a lei aplicável.

Eco Heroes International SL · CIF B44915940 · 17003 Girona (Espanha) · info@eco-heroes.org · https://eco-heroes.org/trust/ · Acordo de Subcontratação v1.7, 25 de outubro de 2026. O modelo publicado é disponibilizado para análise; a versão assinada faz parte da Licença.