本译文仅为方便阅读而提供。英文版本为具有法律约束力的文本，如有任何差异，以英文版本为准。 English (PDF)

数据处理协议

依据《(欧盟) 2016/679号条例》（GDPR）第28条及西班牙12月5日《关于个人数据保护和数字权利保障的第3/2018号组织法》（LOPDGDD）第33条订立 — 由许可持有人（“控制者”）与 Eco Heroes International SL（“处理者”）签订

当事方及角色

控制者：_____（许可协议中载明的学校、学校集团、教育主管部门、企业或酒店名称），注册地址 _____，代表人 _____（姓名、职务）。
控制者的数据保护联系人（管理员联系人，或已任命的数据保护官）：_____。

处理者：Eco Heroes International SL，税号（CIF）B44915940，注册办事处位于 17003 Girona（西班牙），在 Registro Mercantil de Girona 登记，代表人为创始人 Karim Zouhdi。数据保护联系方式：info@eco-heroes.org，+34 690 814 215。安全报告：security@eco-heroes.org（见 https://eco-heroes.org/.well-known/security.txt）。

角色。控制者决定处理控制者数据的目的和方式，是该等数据的控制者。处理者仅代表控制者处理控制者数据，是 GDPR 第4条第(8)项所指的处理者。

教师账户。每位教师都有一个以本人姓名开设的个人账户。处理者依据其隐私政策，作为控制者运营账户本身（登录、安全、两步验证和免费教师资料）。教师在服务中为控制者所做的一切均属于控制者数据：账户在控制者组织中的角色和权限、班级、学生、学习进度、作业、实时测验、名册导入、从学习平台启动以及影响研究。

不属于本协议范围的内容。附件一B部分列出处理者本身作为控制者的处理活动。这些活动受处理者隐私政策（https://eco-heroes.org/legal/privacy/）而非本协议的约束。Eco Heroes Academy（learn.eco-heroes.org）和 VSME 评估（assessment.eco-heroes.org）是另行提供的服务，有各自的条款和隐私说明；本协议不适用于这两项服务。

本协议构成许可协议的组成部分。如许可协议与本协议在个人数据处理方面存在冲突，以本协议为准。

定义

- **“许可协议”**：控制者据以使用服务的协议，即控制者接受的报价单或订单，连同发布于 https://eco-heroes.org/legal/licence/ 的《学校和机构许可条款》。
- **“服务”**：第1.1条所述的 Eco Heroes 平台及支持服务。
- **“控制者数据”**：处理者依据本协议代表控制者处理的个人数据，详见附件一A部分。

- **“用户”**：经控制者允许使用服务的学生、教师、学校管理员、教职员工、雇员、住客及其他人员。
- **“次级处理者”**：处理者为处理控制者数据而聘用的另一处理者。
- **“工作日”**：星期一至星期五，Girona（西班牙）的公众假日除外。
- GDPR 第4条所定义的术语，例如“个人数据”、“处理”和“个人数据泄露”，在本协议中具有相同含义。

1. 标的与期限

1.1 处理者依据许可协议向控制者提供服务。服务包括：冒险游戏、知识问答、文字游戏和课堂实时测验；绘本和故事图书馆、任务视频、手册和课程活动页；以本人姓名开设的教师账户、班级管理和作业；可选的名册导入（CSV、OneRoster CSV、Google Classroom）；可选的通过 Google 或 Microsoft 进行的教师登录；可选的通过 LTI 1.1 或 LTI 1.3 与控制者学习平台的连接；控制者使用时的 Eco Heroes 移动应用班级仪表板；可选的影响研究；企业和酒店许可下的协调员账户、为员工或住客子女设立的带访问码的小组以及按小组生成的进度报告（CSV）、机构汇总报告、带有机构名称的证书，以及员工可选择通过控制者自己的身份提供商登录；以及支持服务。

1.2 处理者在许可协议有效期内，并直至所有控制者数据依据第10条被删除或返还为止，处理控制者数据。

2. 处理的性质和目的；类别

2.1 处理的性质和目的、数据主体的类别以及个人数据的类别载于**附件一**。

2.2 处理者仅为向控制者提供服务之目的处理控制者数据。处理者不将控制者数据用于广告，不用于建立超出服务向控制者教师所展示的学习进度范围的学生画像，不用于出售或出租数据，也不用于开发服务以外的产品。

2.3 **匿名统计。**控制者将班级登记参加影响研究时，即指示处理者根据作答编制汇总统计，处理者可在其自身的报告和出版物中使用该等统计。处理者仅汇总至少10名学生组成的小组的作答，绝不纳入自由文本作答，并核实无法识别任何学生、班级或学校。以此方式编制的统计不再属于个人数据。控制者可随时书面通知撤回该指示；此后收集的作答仅用于控制者自身的结果。

3. 指示

3.1 处理者仅根据控制者的书面指示处理控制者数据，包括向第三国或国际组织传输数据，但处理者所适用的欧盟或成员国法律要求进行处理的除外；在此情况下，处理者应在处理前将该法律要求告知控制者，除非该法律基于重要的公共利益理由禁止提供此类信息。

3.2 控制者的书面指示包括本协议、许可协议以及控制者及其用户在服务中所作的设置选择（例如：创建班级、导入名册、启用单点登录或学习平台连接、将班级登记参加影响研究、删除学生或班级）。其他指示由控制者的管理员联系人以书面形式发出；发送电子邮件至 info@eco-heroes.org 即可。

3.3 如处理者认为某项指示违反 GDPR、LOPDGDD 或其他欧盟或成员国数据保护规定，应立即告知控制者。处理者可暂停执行该指示，直至控制者确认或修改该指示。

4. 控制者的义务

4.1 控制者负责：处理的合法性，包括处理学生数据的法律依据；向数据主体（学生及在适用情况下其父母或监护人、教师、管理员、雇员和住客）提供 GDPR 第13条和第14条要求的信

息；针对未达数字同意年龄的学生取得控制者所适用法律要求的同意（GDPR 第8条；LOPDGDD 第7条：在西班牙为14岁）；以及控制者及其用户所输入数据的准确性。

4.2 控制者应要求其用户不得在自由文本字段（例如昵称、班级名称、作业备注、实时测验昵称和调查作答）中输入特殊类别的个人数据（GDPR 第9条）、学生的姓氏、电子邮件地址或其他直接标识符。

4.3 控制者连接其自身的学习平台（LTI）或身份提供方（单点登录）时，应对该系统及其配置负责，使其仅共享附件一所述的数据（通过 LTI 进入的学生仅共享姓名，绝不共享电子邮件地址）。

4.4 控制者应指定一名管理员联系人，并在开展影响研究之前指定一名儿童保护（安全保障）联系人，并在服务中或通过向处理者发送电子邮件使两名联系人的信息保持最新。在指定儿童保护联系人之前，或指定联系人的账户关闭期间，服务将儿童保护提示转交控制者的学校管理员。对于在服务中未关联任何学校的班级（例如仅通过 LTI 启动使用的班级），提示转交处理者的儿童保护负责人，由其毫不迟延地转交控制者的管理员联系人。

5. 处理者的义务

处理者应：

a. 仅依据第3条处理控制者数据；

b. 确保获授权处理控制者数据的人员已承诺保密或负有适当的法定保密义务，并将对生产系统的访问限于确有需要的指定人员；

c. 实施**附件二**所列的技术和组织措施，并考虑到数据主体包括儿童，依据 GDPR 第32条维持与风险相适应的安全水平；

d. 仅按照第6条的条件聘用其他处理者；

e. 考虑到处理的性质，在可能的范围内通过适当的技术和组织措施，协助控制者履行答复数据主体行使权利请求的义务（GDPR 第12条至第23条），具体见第8条；

f. 考虑到处理的性质以及处理者可获得的信息，协助控制者确保遵守 GDPR 第32条至第36条（安全、泄露通知、数据保护影响评估、事先咨询）；处理者现行数据保护影响评估的摘要已在信任中心公布，完整评估应控制者要求提供；

g. 在服务结束时，按照控制者的选择删除或返还全部控制者数据，并删除现有副本，但欧盟或成员国法律要求保存数据的除外（第10条）；

h. 向控制者提供证明其遵守 GDPR 第28条所需的一切信息，并允许和配合控制者或其授权的其他审计人员进行审计，包括检查（第11条）；

i. 保存代表控制者进行的所有类别处理活动的记录（GDPR 第30条第2款）；

j. 仅按照第7条的条件将控制者数据传输至第三国。

6. 次级处理者

6.1 控制者对**附件三A部分**所列的次级处理者给予一般书面授权。

6.2 处理者拟增加或更换次级处理者时，应至少提前**30天**通过向控制者管理员联系人发送电子邮件并更新 https://eco-heroes.org/trust/ 的方式通知控制者。控制者可基于合理的数据保护理由提出异议。如异议在通知期内未能解决，控制者可无须支付违约金终止许可协议的相关部分，并适用第10条。

6.3 处理者依据各提供方的标准数据处理条款聘用各次级处理者。该等条款对次级处理者施加数据保护义务，就适当的技术和组织措施提供充分保证，符合 GDPR 第28条第4款的要求。处理者就各次级处理者履行该等义务向控制者承担全部责任。

6.4 **附件三B部分**列出处理者使用但**不**处理控制者数据的第三方服务。这些服务不处理个人数据，或仅处理处理者本身作为控制者的数据。列出这些服务是为了透明，它们不是本协议所指的次级处理者。

6.5 控制者自身的系统，例如其学习平台或其 Google 或 Microsoft 环境，由控制者选择和管理，不是处理者的次级处理者。

7. 国际传输

7.1 控制者数据在欧盟境内托管和存储：应用服务器位于法国（Internet Girona，基于 OVHcloud 基础设施）；数据库、加密备份和备用服务器位于德国和芬兰（Hetzner Online GmbH）。内容分发网络（Cloudflare）从其全球网络提供已缓存的公开页面。含有个人数据的响应被标记为私有且不可存储（no-store），该网络不会缓存这些响应。

7.2 处理者不将控制者数据传输至欧洲经济区以外，也不允许任何次级处理者这样做，除非：(i) 欧盟委员会已就目的地作出充分性认定，包括瑞士以及处理者已在官方名单上核实其认证的组织所适用的欧盟—美国数据隐私框架；或 (ii) 依据委员会第(EU) 2021/914号实施决定通过的标准合同条款（模块3，处理者至处理者，或在适用时为模块2），并在传输影响评估表明有必要时辅以补充措施。附件三载明适用于各次级处理者的保障措施。处理者为欧洲经济区以外的每一次级处理者保存书面传输影响评估，并应控制者要求提供。

7.3 Cloudflare, Inc. 在其网络边缘终止加密连接，因此在该处处理请求数据（IP 地址、所请求的地址、标头）。处理者依据含有标准合同条款的 Cloudflare 标准数据处理条款，并在 Cloudflare 列入数据隐私框架官方名单时依据欧盟—美国数据隐私框架。

7.4 Proton AG 在瑞士托管处理者的电子邮件。欧盟委员会已就瑞士作出充分性认定。

8. 协助数据主体行使权利

8.1 教师可直接在服务中查看、导出（CSV）、重命名、重置和删除学生数据，并可删除整个班级。每位教师只能看到自己的班级；学校管理员可看到本校所有班级，并可立即撤销某位教师的访问权限。控制者在可能时使用这些功能答复请求。

8.2 如请求无法通过服务完成，处理者应在收到书面请求后**10个工作日**内协助控制者。如处理者直接收到数据主体（包括父母或监护人）关于控制者数据的请求，处理者不就请求的实质内容作出答复；除控制者另有指示外，处理者应无不当延迟地将数据主体转介给控制者，并通知控制者。

9. 个人数据泄露

9.1 处理者在知悉影响控制者数据的个人数据泄露后，应无不当延迟地，且最迟在**48小时**内通知控制者。首次通知应在当时已知的范围内包含 GDPR 第33条第3款要求的信息：泄露的性质、受影响的数据主体和记录的类别及大致数量、可能的后果，以及已采取或拟采取的措施。处理者应在获得更多信息时分阶段补充。

9.2 处理者应与控制者合作调查、控制和记录泄露事件，并协助控制者向监管机构（在西班牙为 Agencia Española de Protección de Datos）进行通报及向数据主体进行通知。处理者应记录每一起个人数据泄露，包括相关事实、影响和已采取的补救措施。

9.3 处理者通过电子邮件向控制者的管理员联系人发送通知。任何人均可向 security@eco-heroes.org 报告安全漏洞。报告将在5个工作日内获确认，严重问题优先于所有其他工作予以修复。

10. 保存、删除和返还

10.1 **许可协议有效期内。**控制者数据按照附件一C部分的计划保存，该计划反映服务代码中实施的保存规则。教师可随时删除学生或班级，删除在运行中的数据库和备用副本中立即生效。

10.2 **导出。**在许可协议有效期内并直至依据第10.3条删除为止，控制者可在服务中将班级和进度数据导出为 CSV，或要求处理者以结构化、常用和机器可读的格式进行导出。

10.3 **许可协议终止。**如许可协议终止且未续订，处理者应在终止日后**90天**删除控制者数据。如控制者书面提出要求，无论许可协议是否已终止，处理者应在收到要求后**30天**内删除控制者数据。处理者应根据要求以书面形式确认删除。删除之前，处理者应在删除日前30天和7天向控制者的学校管理员发送电子邮件，说明该日期以及续订许可协议或导出数据的方式；删除不早于第一封邮件发出后30天、第二封邮件发出后7天。

10.4 **教师账户。**与教师账户关联的最后一项许可终止后，该账户作为免费教师账户继续存在。除非教师在此期间关联到新的许可，该账户将在该许可终止后12个月删除；免费账户在连续12个月未登录后删除。处理者在删除前30天向教师发送电子邮件。教师账户继续存在并不意味着保留任何控制者数据：控制者数据依据第10.3条删除。

10.5 **备份和副本。**已删除的数据在正常周期内从备份中消失。加密备份按轮换方式保留，因此已删除的数据在**14天**内从所有备份中消失。备用服务器上的只读副本持续同步每一次删除。备份仅为弥补生产系统的损失而恢复；如恢复使已删除的数据重新出现，将再次执行删除。

10.6 **法定保存。**许可协议终止后，处理者仅在欧盟或成员国法律要求的范围和期限内保存个人数据，例如依据西班牙《商法典》（Código de Comercio）第30条将发票和会计记录保存6年。这些记录可识别控制者的联系人，不含任何学生数据。处理者依据附件二保护这些记录，不将其用于其他目的。

11. 审计和信息

11.1 经要求，处理者每个合同年度至多一次（另在发生个人数据泄露后或存在有据可查的、合理的不合规怀疑时）向控制者提供证明遵守本协议所需的信息，包括现行安全摘要（https://eco-heroes.org/trust/#security）、现行次级处理者名单、代表控制者进行处理的记录、传输影响评估、数据保护影响评估、最近的恢复测试和故障切换演练结果，以及已进行的安全审查结果。

11.2 如上述信息不足，控制者或经其授权并负有保密义务的独立审计人员可至少提前**30天**通知，在正常工作时间内，在不对处理者的运营或其他客户造成不合理干扰的情况下，审计处理者的相关处理活动。各方自行承担费用。处理者可要求审计人员签署合理的保密协议，并可将对与其他客户共享的系统的访问限于核实合规所必需的范围。

12. 责任

12.1 各方依据 GDPR 第82条对数据主体承担责任。双方之间的责任受许可协议的责任条款约束。本协议或许可协议的任何内容均不限制法律不允许限制的一方责任，包括故意行为的责任。

12.2 如处理者因控制者的指示或因控制者未履行第4条规定的义务而须支付行政罚款或损害赔偿，控制者应在该原因所及的范围内赔偿处理者，反之亦然。

13. 期限、适用法律和管辖

13.1 本协议自许可协议开始之日起生效，并在所有控制者数据依据第10条被删除或返还时终止。第5条(b)项、第10条、第11条和第12条在必要期间内继续有效。

13.2 本协议受西班牙法律以及包括 GDPR 和 LOPDGDD 在内的欧盟法律管辖。Girona（西班牙）的法院具有管辖权，但不影响控制者作为公共机构或依据公共采购法所适用的强制性规定，也不影响数据主体依据 GDPR 第79条享有的权利。附件五补充适用于英国和美国控制者的规定。

13.3 对本协议的变更须以书面形式作出；电子邮件即可。处理者在 https://eco-heroes.org/trust/ 发布现行范本。范本的新版本未经控制者同意不改变已签署的协议。控制者的学校管理员可在线接受本协议；处理者记录接受人、接受时间、所接受的版本以及所用 IP 地址的密钥哈希。

签署

控制者代表	处理者代表 — Eco Heroes International SL
姓名、职务	Karim Zouhdi，创始人
日期、签名	日期、签名

附件一 — 处理说明

A. 代表控制者进行的处理（本协议适用范围）

附件一A — 代表控制者进行的处理

项目	说明
标的	依据许可协议向控制者的用户提供服务。
性质	数据的托管、存储、显示和删除；进度记录；课堂实时测验；作业；证书；班级管理；可选导入控制者提供的名册（粘贴或上传 CSV、OneRoster CSV 1.1/1.2、Google Classroom）；可选的从控制者学习平台进行的 LTI 1.1 / LTI 1.3 启动，含 Names and Role Provisioning（名册导入）和 Assignment and Grade Services（成绩回传）；根据控制者的选择可选通过 Google 或 Microsoft 进行的教师登录；控制者分发班级码时的 Eco Heroes 移动应用班级仪表板；在控制者登记的班级中可选的影响研究问卷；企业和酒店许可下的协调员账户、小组访问码和按小组生成的进度报告（CSV）；支持服务。对于企业和酒店许可，另外还包括：为机构提供汇总的活动报告（机构报告和汇总数据，基于少于 5 个家庭的数字一律隐藏）以及可选的团队排行榜；在孩子的证书上显示机构名称和标志；员工可选择通过控制者自己的身份提供商登录（OpenID Connect）。
目的	依据联合国可持续发展目标提供可持续发展教育，并按许可协议的规定进行进度记录、报告和评估。就影响研究而言：控制者对其自身教学的评估（供控制者教师查看的班级结果），以及依据第2.3条形成的匿名汇总统计。无其他目的。
数据主体类别	学生（游戏面向9至17岁，分为9–12岁和13–17岁两个年龄组；可打印的课程活动页适用于6–10岁、11–13岁和14–17岁三个阶段，控制者可自行决定将服务用于更年幼的学生）；教师；学校管理员；仅在使用同意流程时的父母和监护人；企业和酒店许可下员工或住客的子女以及机构的协调员。
个人数据 — 学生（网站，在班级中）	学生或教师输入的名字或昵称（2–24个字符；通过名册导入时为名字加姓氏首字母，仅为区分同名的两名学生才扩展至姓氏的前3个字母 — 绝不使用全名）；在游戏中选择的年龄组（9–12岁或13–17岁）；从固定集合中选择的头像；语言；进度（积分、已完成的目标和任务、测验星级、按主题统计的作答数和答对数）；已完成的作业；加入日期和最后活动日期；存储在学生设备上、用于保存进度的随机班级令牌。在课堂实时测验中：输入的昵称、作答、作答时间和得分。不收集：电子邮件地址、姓氏、照片、出生日期、邮寄地址、位置、设备或广告标识符。
个人数据 — 学生（LTI 启动）	平台用户标识符的密钥哈希（用于将学生与席位关联）；仅在平台授予成绩服务访问权限时于启动记录中保存90天的平台用户标识符（成绩回传所需）；作为昵称的名字和姓氏首字母；课程标识符和课程名称；角色；区域设置；最后提交的分数。不存储电子邮件地址和全名；控制者应将其平台配置为仅共享姓名。
个人数据 — 学生（移动应用，班级仪表板）	活动（所玩的每日游戏、日期、语言、得分、是否完成、用时；达成的目标、徽章）以及应用生成的随机安装标识符的单向哈希。学生以生成的别名向教师显示。对活跃学生少于五名的班级，仪表板不显示任何内容。

项目	说明
个人数据 — 学生（控制者登记班级时的影响研究）	对研究问卷的作答（选项、评分和可选的简短自由文本）、问卷版本、语言、年龄组、开始和提交时间以及质量标记。电子邮件地址和电话号码在接收时从自由文本中删除。可能包含与儿童保护相关的倾诉的作答会提示给控制者指定的联系人。各轮研究之间的作答通过学生在班级中席位的单向密钥哈希关联；不收集姓名、电子邮件地址或出生日期。每个席位上由控制者记录的异议或书面同意。如未指定儿童保护联系人，则由第4.4条规定的接收人代替。
个人数据 — 教师和学校管理员	姓名、工作电子邮件地址、学校、角色（教师或学校管理员）、语言；密码（bcrypt 哈希）或单点登录标识符；如已启用，两步验证密钥和经哈希处理的备用码（学校管理员必须启用）；电子邮件验证状态；登录时间和次数；会话；创建的班级；名册导入预览（仅姓名，在会话中保留30分钟）；管理操作审计日志记录（含 IP 地址的密钥哈希，以及由内容分发网络提供、以两个字母代码表示的连接国家）；支持往来信件。
个人数据 — 教师（影响研究）	教师问卷的作答，以及针对6–8岁儿童的班级观察表，通过教师账户或代码的单向密钥哈希关联；班级的登记、其同意形式以及在研究中的分组。
个人数据 — 父母和监护人	仅在网站的家长同意流程用于未达数字同意年龄的学生时：父母电子邮件地址的单向密钥哈希（地址本身仅用于发送一次确认链接，不予存储）、决定及其时间戳。
个人数据 — 子女和协调员（企业和酒店许可）	控制者员工或住客的子女：他们在自己的设备或家庭设备上，使用控制者的访问码和一个英雄名（昵称）加入小组，没有账户，也没有电子邮件地址。服务存储与班级学生相同的数据：英雄名、年龄组、头像、语言、进度和测验结果。协调员：姓名、工作电子邮件地址、密码哈希或登录标识符、两步验证设置以及其创建的小组。协调员可按小组查看已完成的目标和测验结果，并可将其导出为 CSV。为生成机构报告，本服务还会为这些小组中的每个英雄档案记录活跃日期以及首次完成每个目标或任务的日期（精确到日；学校班级不会这样记录）。报告只包含汇总数据：不含姓名、昵称、标识符或按孩子逐行的数据；基于 1 至 4 个家庭的数字一律隐藏（k = 5），如果仅凭一个数字就能推算出被隐藏的数字，则另一个数字也会隐藏。团队名称由控制者的管理员选定，不得指名道姓。控制者开启企业账号登录时，员工的姓名和邮箱地址来自控制者自己的身份提供商（范围为 openid、email 和 profile）；该身份提供商是控制者自己的系统和受托处理者，不是次级处理者，其主体标识符仅以密钥哈希形式保存。联合品牌：机构的显示名称和标志，由控制者提供。家长或监护人可在 LinkedIn 上分享的公开徽章页面不含任何个人数据（只有目标数量、控制者选择开启时的机构名称以及一种语言，均取自其链接）；分享由成年人发起，处理者不会向 LinkedIn 发送任何信息。
特殊类别（GDPR 第9条）	不要求，也不需要。见第4.2条。
频率	在许可协议有效期内持续进行。

B. Eco Heroes 作为独立控制者进行的处理（不属于本协议范围）

列出以便控制者了解本协议的边界。这些处理受处理者的隐私政策（v4.3）和儿童隐私声明（v2.2）约束，而非本协议：

- **教师账户本身：** 登录、安全、两步验证和免费教师资料。处理者是账户本身的控制者，并依据第10.4条删除账户；账户为控制者开展的活动属于控制者数据。

- **免费教师账户：** 未关联任何许可、以已验证的电子邮件地址使用免费教师资料（手册课程和教师指南）的教师。
- **家庭订阅**（由父母或监护人在网站上订购）：电子邮件地址（部分遮盖后存储）、Stripe 的付款和订阅参考信息，以及个人访问码（以密钥哈希存储）。银行卡信息从不到达处理者。在学校使用的家庭码不携带任何学校数据。
- **应用账户**（父母通过 Google 或 Apple 登录；通过 Google Play 或 Apple 订阅；通过 RevenueCat 获取订阅状态）。
- **网站访客**（面向成人的公开页面：经同意后的 Google Analytics 4；通过 Formspree 的联系表单；通过处理者自有服务器提交的报价请求和大使申请；通过 Brevo 发送的 Dinner Questions 邮件）。
- **测验公开排行榜**（可选：从生成列表中选取的昵称、得分和 IP 地址的密钥哈希；保存30天）。
- **项目调查：** 由处理者在班级以外开展，在法律要求时取得父母同意。
- **另行提供的服务：** Eco Heroes Academy（learn.eco-heroes.org）和 VSME 评估（assessment.eco-heroes.org）有各自的条款和隐私说明。

C. 保存计划（按服务中的实施情况）

附件一C — 保存计划

数据	保存期限	机制
学生数据以及企业和酒店小组中儿童的数据（昵称、年龄组、头像、进度、作业、应用中的班级活动、LTI 席位关联）	许可协议有效期内：直至教师或管理员删除该学生或班级。许可协议终止后：除非续订，否则在终止日后90天删除。经控制者书面要求：在30天内删除；删除前30天和7天以电子邮件通知学校管理员	教师或管理员在服务中的操作；许可终止时自动删除；处理者根据书面要求处理
企业和酒店小组中英雄档案的活跃日期（机构报告）	与英雄档案一同保存，并按上述规则随档案一同删除	随档案删除
机构设置：团队名称和各小组所属团队、团队排行榜设置、联合品牌的名称和标志、企业账号登录配置	在许可期内；应控制者要求删除	处理者应要求执行
企业账号登录：登录流程记录；已固定的身份关联（身份提供商主体的密钥哈希）	流程记录：使用后或 10 分钟后删除。身份关联：直到账号被删除，或控制者的登录配置被删除或重置为止	自动清除；管理员操作
课堂实时测验（昵称、作答、时间、得分）	测验会话创建后30天	每日自动清理
名册导入预览（OneRoster）	30分钟，仅在教师的服务器会话中	会话过期
Google Classroom 访问令牌（名册导入）	仅在导入期间，保存在教师会话中；从不写入数据库	会话过期
LTI 启动记录	教师启动和无成绩服务的学生启动：2小时。有成绩服务的学生启动：90天	LTI 活动时自动清理
LTI 登录状态、交接令牌、深度链接令牌、随机数、名册导入令牌	10分钟 / 10分钟 / 60分钟 / 15分钟 / 2小时	自动清理；一次性使用

数据	保存期限	机制
教师、协调员和学校管理员账户	与账户关联的最后一项许可终止后12个月；免费账户在连续12个月未登录后；删除前30天发送提醒邮件。未验证的注册：最后一个确认链接过期7天后删除	账户自动清理
会话和“保持登录”	按配置时长保留的服务器会话，在登录时及每30分钟更新；更改密码或管理员撤销访问权限时终止所有会话。“保持登录” Cookie：180天（HMAC 签名）	代码
速率限制记录（登录尝试及其他限制）	30天	每日自动清理
安全审计日志（管理操作、访问码激活和登录；IP 的密钥哈希、以两个字母代码表示的连接国家）	12个月	每日自动清理
调查作答和同意请求中的防滥用 IP 哈希	30天（作答本身按其自身期限保存）	每日自动清理
家长同意请求	未答复或已过期：30天。拒绝：12个月。已给予的同意：在依赖该同意期间；同意撤回时连同数据一并删除	每日自动清理；删除功能
影响研究作答（学生、教师、观察表）以及异议或同意标记	研究最后一轮结束后24个月；如控制者书面指示则更早。异议和同意标记随班级登记一并删除	每日自动清理；处理者根据书面要求处理
儿童保护提示（可能包含倾诉的影响研究作答，以及其所属的席位和昵称）	作答文本在提示标记为已处理后30天删除；提示记录在处理后12个月删除	每日自动清理
项目调查作答	24个月，或直至同意被撤回	每日自动清理；删除功能
测验公开排行榜记录（不属于本协议范围，为完整起见列出）	30天	每日自动清理
控制者接受本协议的记录（接受人、时间、版本、IP 地址的密钥哈希；由处理者作为控制者保存，第13.3条）	许可有效期内及许可结束后6年	处理者的记录
家庭计划的结账接受、取消和撤销记录（不属于本协议范围，为完整起见列出）	与会计记录一并保存6年（西班牙《商法典》第30条）	会计记录
源自个人的参与率计数器	2天	每日自动清理
遥测（CSP 违规和 JavaScript 错误报告）	不存储标识符（截短的用户代理）；速率计数器每分钟重置；日志上限为 5 MB	代码
支持往来信件（电子邮件）	直至请求处理完毕，最长为最后一封信件后12个月	处理者邮箱处理程序
加密备份	加密备份按轮换方式保留；已删除数据在14天内从所有备份中消失	自动

数据	保存期限	机制
数据库备用副本	持续；同步每一次删除	复制
Web 服务器技术日志（IP 地址、所请求的地址）	最长90天	服务器配置
发票和付款记录	6年（西班牙《商法典》第30条）；可识别控制者的联系人，从不识别学生	会计记录

附件二 — 技术和组织措施（GDPR 第32条）

截至本协议签订之日有效的措施。每次发布时进行审查，现行摘要发布于 https://eco-heroes.org/trust/#security。处理者可更新这些措施，但整体安全水平不得降低。

1. 传输加密

- 所有连接使用 TLS 1.2 或更高版本；HTTP Strict Transport Security，max-age 为两年，并启用 includeSubDomains 和 preload；证书自动续期；内容分发网络与服务器之间使用源站证书。
- 应用服务器仅通过 TLS 1.2/1.3 连接数据库，并依据固定的证书颁发机构验证证书；数据库拒绝未加密的连接（require_secure_transport）。数据库账户限于应用主机和备用主机。
- 备份在离开服务器前进行加密（AES-256-CBC，PBKDF2 迭代200,000次），并仅通过加密连接发送。不写入任何未加密的归档。

2. 浏览器端保护

- Content-Security-Policy：内联脚本仅在通过逐个脚本的 SHA-256 哈希获得批准，或在少数动态页面上带有每次请求生成的随机数时才会运行（脚本不使用 unsafe-inline — 仍允许内联样式；object-src 'none'，base-uri 'self'，frame-ancestors 'none'，但仅允许已注册学习平台嵌入的 LTI 页面除外）。违规报告在速率限制下收集。儿童页面不加载任何第三方脚本。在成人页面上，第三方脚本仅限经同意后的 Google Analytics，以及登录和注册表单上的 Cloudflare Turnstile 验证。
- 网页字体托管在处理者自有的服务器上。不向 Google Fonts 或其他字体提供方发送请求。
- 安全标头：X-Content-Type-Options: nosniff、X-Frame-Options: DENY、Referrer-Policy、Permissions-Policy、Cross-Origin-Opener-Policy 和 Cross-Origin-Resource-Policy same-origin。删除服务器和 PHP 版本标头。拒绝 HTTP TRACE 和 TRACK。
- Cookie：会话 Cookie 设置为 Secure、HttpOnly 和 SameSite=Strict，采用严格会话模式；会话 ID 在登录时、激活代码时以及每30分钟更换一次。“保持登录” Cookie 使用服务器端密钥进行 HMAC 签名。LTI 状态 Cookie 限于 /lti/ 路径并进行分区。
- 游戏的 Service Worker 从不缓存标记为 no-store 或 private 的响应，也不缓存仅限会员的路径，因此在共享设备上注销后不会有受保护的内容留在缓存中。
- 含有个人数据或仅限会员内容的响应以 Cache-Control: private, no-store 发送，内容分发网络从不缓存这些响应。

3. 访问控制和身份验证

- 以本人姓名开设的教师账户：学校代码仅在注册时使用一次。它会创建一个带有已验证电子邮件地址的本人账户，或将学校关联到教师的现有账户。此后，教师使用本人的电子邮件地址和密码或通过单点登录进行登录。仅输入了学校代码的设备可以玩游戏，但没有教师工具。管理员代码仅用于创建学校的第一个管理员账户，该账户确认后即失效；此后，教师使用学校管理员在本服务中创建的教职工代码加入，该代码仅显示一次，仅以密钥哈希形式存储，并可随时更换。
- 教师密码使用 bcrypt 进行哈希处理，并以恒定时间进行比较。首次登录前须验证电子邮件地址。更改密码会终止所有会话。学校管理员可立即撤销某位教师的访问权限。
- 两步验证（TOTP，附带经哈希处理的备用码）对学校管理员和处理者的超级管理员为强制要求，任何教师以及企业和酒店许可的协调员均可启用。注册用二维码在服务器上生成，因此密钥从不离开服务器。第二因素在创建会话之前进行验证，学校管理员在任何可见学生数据的地

方都必须使用。儿童保护联系人阅读儿童保护提示时也必须使用。24 小时内输错 10 次代码后，该账户的第二因素将锁定 15 分钟，并通过电子邮件通知账户持有人。

- 访问码仅以密钥哈希形式存储在 Web 根目录之外的文件中；密钥保存在 Web 根目录之外。注册码和许可码以相同方式存储；代码仅在创建时显示一次。
- 对登录（按 IP 地址以及按电子邮件和 IP 组合，并设有总体上限）、注册、兑换代码、加入班级、加入实时测验、同步进度、报价表单、LTI 登录、遥测端点和 Stripe 返回查询实施速率限制。所有修改数据的表单均使用 CSRF 令牌。对所有 next= 参数防范开放重定向。
- 访问权限在服务器端校验：仅限会员的资源（任务视频、测验题库、图书、LTI 内容）仅在服务器校验有效的代码会话、已签名的记住代码或已登录账户后才提供。浏览器自行写入的任何内容均不授予访问权限。
- 按角色和学校隔离：每位教师只能看到自己的班级；学校管理员可看到本校所有班级，看不到其他学校的任何内容；通过 LTI 进入的教师只能看到其启动所在课程的班级；超级管理员访问权限限于处理者的指定员工。
- 所有数据库查询均使用预处理语句；不使用 exec、eval 或 unserialize；文件路径仅由许可列表中的元素构建；上传文件（名册 CSV/ZIP 文件、调查图片）有大小限制、经类型检查并存储在 Web 根目录之外；关闭 PHP 错误显示。
- 为企业和酒店员工提供可选的单点登录，采用 OpenID Connect（带 PKCE 的 Authorization Code；对签名的 ID 令牌校验签发者、受众、有效期和 nonce）。客户端密钥加密存储。账号只在控制者允许的邮箱域名范围内匹配，绝不会关联到其他机构的账号。

4. 数据最小化和儿童数据

- 不收集学生的电子邮件地址、姓氏、照片、出生日期、邮寄地址、位置或设备或广告标识符。名册导入仅保留名字和姓氏的前3个字母。通过 LTI 进入的学生以平台用户标识符的密钥哈希及名字和姓氏首字母存储；控制者应将其平台配置为仅共享姓名。
- IP 地址仅以密钥哈希（前缀）形式存储。持有密钥者可以重新关联这些数据，因此它们是假名化的，而非匿名的。当其附随于内容时，在30天后删除。
- 儿童页面（/game、/games、/trivia、/library、/sdg、/wordle、/missions、/books 及其各语言版本）不加载任何分析工具，也不显示同意横幅。在其他页面上，仅在明确同意后才加载分析工具。
- 仅限会员的任务视频由处理者托管，并在校验访问权限后提供。仍使用 YouTube 播放器的地方（免费游戏）使用 youtube-nocookie.com，且仅在用户点击播放时才加载。
- 在测验公开排行榜上发布成绩是每局游戏结束后的可选项，使用生成的昵称（一个形容词加一种动物；不允许自由文本，不显示学校）。公开排行榜显示最近30天前10名的昵称和得分，记录在30天后删除。每条公开记录都有举报链接；被举报三次的记录在审核前隐藏。班级排行榜仅对该班教师和学校管理员可见，他们可以删除记录。
- 自由文本作答在提交时自动过滤：删除电子邮件地址和电话号码；与一份可能表明儿童处于危险中的简短词语列表匹配的作答会从研究数据中移出，仅转交学校指定的儿童保护联系人。姓名不会被自动删除；阅读作答的研究人员会标记可能的姓名，并且绝不在报告中提及。可能的倾诉会在一个上课日内转交学校指定的联系人。如未指定儿童保护联系人，则由第4.4条规定的接收人代替。
- 同意流程中父母的电子邮件地址从不以明文存储；仅保留密钥哈希。
- 机构报告为汇总数据：基于少于 5 个家庭的数字在计算过程中即被隐藏，因此屏幕和 CSV 都无法显示。只有使用两步验证登录的机构管理员才能打开；每次查看和导出都有频率限制并会被记录。

5. 可用性、备份和恢复

- 以下各项自动运行。独立监控（UptimeRobot，11项检查，每5分钟一次）在出现故障时向处理者发出警报。
- 每晚对数据库和应用进行加密备份，副本保存在另一个欧盟国家的独立数据中心。每月自动测试一次恢复。
- 每次发布前进行备份，并有经过测试的回滚程序；保留上一个生产版本。
- 备用服务器保存应用的副本和数据库的实时副本。主 Web 服务器发生故障时，带健康检查的负载均衡会自动切换流量；数据库服务器发生故障时，按照脚本化并经过演练的程序提升副本。两者均已于 2026 年 10 月测试。
- 每小时进行一次基础设施检查（副本状态和延迟、证书到期、磁盘空间、待安装的安全更新、内容分发网络地址范围）。操作系统安全更新自动安装。在网络边缘防御 DDoS 攻击和机器人。
- 测试环境与生产环境分离（独立的 Unix 用户、启用 open_basedir 的 PHP 池、独立的数据库实例、已移除机密信息）。

6. 日志记录和监控

- 安全事件（登录失败、兑换代码、管理操作、CSP 违规报告、按保存期限进行的删除和清理）连同 IP 地址的密钥哈希一并记录。安全审计日志保存12个月，速率限制记录保存30天（附件一C部分）。
- 服务的当前状态和每次中断均在公开的状态页面上公布。

7. 组织措施

- 对生产系统的访问限于指定人员。所有管理账户（托管、数据库和备份服务器、内容分发网络和 DNS、源代码仓库、监控、电子邮件）均使用两步验证。服务器访问使用 SSH 密钥。防火墙将对数据库和备用服务器的访问限于处理者自有的主机和内容分发网络的地址范围。
- 变更会自动测试（持续集成；未通过测试的代码不予发布），首先经过测试环境，并在每次发布后在生产环境中进行检查（47项在线检查）。对应用进行并记录静态安全审查（最近一次：2026年10月16日）。
- 渗透测试（2026年10月）：由处理者自己的测试团队对平台进行了结构化的白盒和灰盒测试（身份验证、会话、学校之间的访问控制、支付、文件和数据暴露、速率限制以及边缘缓存）。所有严重、高危和中危问题均已在发布前修复并重新测试。计划委托一家独立公司进行外部渗透测试。
- 漏洞报告渠道公布于 /.well-known/security.txt。报告将在5个工作日内获确认，严重问题优先于所有其他工作予以修复。
- 书面的事件响应程序规定处理者如何发现、控制和记录个人数据泄露，以及如何遵守第9条规定的48小时通知期限。
- 处理者保存代表控制者进行处理的记录（GDPR 第30条第2款），以及针对欧洲经济区以外每一次级处理者的传输影响评估。
- 保存期限在执行该期限的代码中设定，因此公布的期限与实际执行的期限不会不一致。
- 机密信息（受限的 Stripe 密钥、单点登录凭据、哈希密钥）保存在 Web 根目录之外，从不放入源代码仓库。

附件三 — 次级处理者和第三方服务

信任中心（https://eco-heroes.org/trust/#subprocessors）列出相同的两份名单。

A部分 — 处理控制者数据的次级处理者

附件三A — 已授权的次级处理者

次级处理者	工作内容	所在地	传输保障措施
Internet Girona（基于 OVHcloud 基础设施）	网站托管	法国（欧盟）	在欧盟境内；提供方的标准数据处理条款
Hetzner Online GmbH，贡岑豪森（德国）	数据库托管、备用服务器和加密备份	德国和芬兰（欧盟）	在欧盟境内；Hetzner 的标准数据处理条款
Cloudflare, Inc.，旧金山（美国）	内容分发、TLS、防御攻击和机器人、登录和注册表单上的 Turnstile 验证，以及故障时自动切换	全球边缘网络；源站服务器在欧盟境内	含标准合同条款（2021/914）的 Cloudflare 标准数据处理条款；Cloudflare 列入名单时适用欧盟—美国数据隐私框架
Proton AG，日内瓦（瑞士）	托管 info@ 和 security@eco-heroes.org 电子邮件：与控制者工作人员之间的支持和数据保护往来信件	瑞士	欧盟委员会对瑞士的充分性认定；Proton 的标准数据处理条款
Google（Google Ireland Ltd / Google LLC）— 仅登录和 Classroom 导入	仅在控制者启用时：教师登录（姓名、电子邮件地址、标识符；无学生数据）；从 Google Classroom 导入名册（读取一次名字和姓氏，存储为名字加姓氏首字母；访问令牌保留在教师会话中）	欧盟 / 美国	控制者自身的 Google 条款；含标准合同条款的 Google 标准数据处理条款；列入名单时适用欧盟—美国数据隐私框架
Microsoft（Microsoft Ireland Operations Ltd）— 仅登录	仅在控制者启用时：教师登录（仅身份；无学生数据）	欧盟 / 美国	控制者自身的 Microsoft 条款；含标准合同条款的 Microsoft Products and Services DPA；列入名单时适用欧盟—美国数据隐私框架
Google（YouTube，youtube-nocookie.com）	播放仍使用 YouTube 播放器的部分教学视频：隐私增强模式，仅在用户点击播放时加载	欧盟 / 美国	Google 的条款；列入名单时适用欧盟—美国数据隐私框架
Moodle Pty Ltd（MoodleCloud），西澳大利亚	仅在控制者使用 Eco Heroes 课程网站 eco-heroes.moodlecloud.com 而非其自身学习平台时：该网站上的课程账户以及游戏向其报告的进度	基于 Amazon Web Services 的 MoodleCloud 托管	MoodleCloud 的数据处理协议，含适用于向欧洲经济区以外任何传输的标准合同条款（2021/914）

B部分 — 不处理控制者数据的第三方服务

为透明起见列出。涉及个人数据时，适用处理者的隐私政策。账户、验证和服务邮件由处理者自有的邮件服务器发送，该服务器不是第三方。

附件三B — 不属于本协议范围的第三方服务

服务	工作内容	所在地	不属于本协议范围的原因
Stripe	网站家庭订阅的银行卡付款；处理者读取付款和订阅状态	欧盟 / 美国；含标准合同条款的 Stripe 数据处理条款；欧盟—美国数据隐私框架	家庭订阅用户是处理者自己的客户；不向 Stripe 发送任何学校数据
Google Analytics 4	面向成人的公开页面的访问统计，仅在同意后；从不用于儿童页面或教师区域	欧盟 / 美国；含标准合同条款的 Google 数据处理条款；欧盟—美国数据隐私框架	不发送任何控制者数据；处理者是其自身网站统计的控制者
Formspree	转发一般联系表单的消息	美国；提供方的标准数据处理条款（标准合同条款；列入名单时适用欧盟—美国数据隐私框架）	消息属于处理者自身的往来信件；服务不使用
Brevo	面向家庭的 Dinner Questions 邮件（订阅后；仅电子邮件地址）	欧盟	面向家庭的通讯；服务不使用
RevenueCat	应用订阅状态（仅账户标识符和购买记录）	美国；标准合同条款	应用家庭账户；无学校数据
Google Play / Apple App Store	应用内订阅付款，由应用商店收取	欧盟 / 美国	应用商店作为独立控制者销售订阅
Google / Apple（应用登录）	应用中父母的可选登录（电子邮件地址和登录标识符）	欧盟 / 美国；欧盟—美国数据隐私框架、标准合同条款	应用家庭账户；无学校数据
UptimeRobot	检查公开页面和状态端点是否响应	欧盟 / 美国	不处理任何个人数据

附件四 — 儿童数据

本附件就18岁以下学生补充附件一和附件二。

1. **数字同意年龄。** 如控制者所适用的法律就直接向儿童提供的信息社会服务要求取得同意（GDPR 第8条），由控制者取得并记录该同意。该年龄在西班牙为14岁（LOPDGDD 第7条），在其他欧盟成员国为13–16岁，在英国为13岁；美国学校见附件五。如控制者以其他法律依据（例如为公共利益执行任务）作为学校使用的基础，则无需同意，由控制者向学生和父母提供信息。服务不核实年龄。其两个年龄组（9–12岁和13–17岁）仅用于选择内容和视频版本。
2. **网站家长同意流程。** 当网站某项功能需要为未达数字同意年龄的儿童取得父母同意时，在父母通过电子邮件发送的一次性链接确认之前，服务不存储任何内容。仅存储父母电子邮件地址的密钥哈希、决定及时间戳。未答复的请求在30天后删除，拒绝在12个月后删除。撤回同意将删除基于该同意收集的数据。
3. **家庭计划。** 父母或监护人订购家庭订阅，成为处理者的客户。在网站上，结账时要求购买人确认已成年；在应用中，登录和购买设置在成人验证（需输入的算术题）之后。两者均不是身份或年龄核验。儿童不在网站上创建账户。儿童可在父母负责的情况下使用家庭码；家庭码不关联任何学校数据。
4. **不进行画像分析，不投放广告。** 处理者不展示广告，不使用广告标识符或广告 SDK。处理者不建立超出控制者教师所查看的进度记录范围的学生画像，不作出产生法律效果或类似重大影响的自动化决策，也绝不为广告目的出售或共享学生数据。
5. **儿童页面不进行分析。** 儿童页面（冒险游戏、游戏合集、测验、图书馆、目标页面、Wordle、任务和图书，全部13种语言）不加载分析工具、追踪器或同意横幅。仅使用严格必要的浏览器存储（语言、设备上的进度、会话）。
6. **影响研究。** 控制者将班级登记参加影响研究时，学生在课堂上作答，作为控制者自身教学评估的一部分。控制者事先告知父母并给予其提出异议的机会，或在其法律或规定要求时取得书面同意；服务支持这两种方式并排除相关席位。学生可以跳过任何问题，并在第一页上获知这一点。教师只能看到班级结果，且仅在至少10名学生在前测和后测中都作答后才能看到；学校中没有任何用户能看到某个学生的个人作答。可能包含与儿童保护相关的倾诉的自由文本作答会转交控制者指定的联系人，由其决定如何处理。处理者依据第2.3条仅使用汇总和匿名的结果，绝不使用自由文本。可能的倾诉会在一个上课日内转交指定的联系人，且只有该联系人能看到。如未指定儿童保护联系人，则由第4.4条规定的接收人代替。
7. **无通信功能。** 服务没有聊天、消息或公开的学生个人资料。测验公开排行榜为可选项，仅使用生成列表中的昵称，不显示学校名称，记录保存30天，且每条记录都有举报链接。班级排行榜仅对该班教师和学校管理员可见，被举报三次的公开记录在审核前隐藏。
8. **告知控制者的剩余风险。** 知道班级码和某学生昵称的同学可以在另一台设备上打开该学生的进度。教师可随时查看、重命名或移除学生，并可更换班级码。控制者应在其自身的评估以及分发班级码的方式中考虑这一点。
9. **父母和学生的权利。** 父母和学生向控制者行使其权利。控制者的教师可以直接查看、导出、重命名、重置和删除学生数据。处理者将其收到的任何请求转交控制者（第8.2条）。
10. **面向儿童的信息。** 处理者在 https://eco-heroes.org/legal/children/ 发布儿童隐私声明，其中一部分写给儿童（A部分），一部分写给父母和学校（B部分）。控制者可在其向学生和父母提供的信息中使用该声明。

附件五 — 英国和美国的控制者

1. **英国。** 如控制者设立于英国，本协议中对 GDPR 的提述应理解为对 UK GDPR 和 Data Protection Act 2018 的提述，主管监管机构为 Information Commissioner's Office（ICO）。控制者数据依据英国针对欧洲经济区的充分性规定从英国传输至欧洲经济区。向美国的再传输在提供方获得认证时依据欧盟—美国数据隐私框架的英国扩展，否则依据标准合同条款的 UK International Data Transfer Addendum。处理者在设计服务时考虑了 ICO 的 Age Appropriate Design Code；其合规摘要见隐私政策第11节。
2. **美国 — FERPA。** 如控制者是受 Family Educational Rights and Privacy Act 约束的美国学校或学区，处理者作为依据 34 CFR 99.31(a)(1)(i)(B) 具有正当教育利益的“school official”行事。处理者在教育记录的使用和维护方面受控制者的直接控制，仅为许可协议的目的使用这些记录，除向第6条所述的次级处理者提供或法律要求外，不向他人披露。
3. **美国 — COPPA。** 对于13岁以下的学生，控制者可在联邦贸易委员会指南允许的情况下，代表父母同意收集附件一所述的数据，因为这些数据仅用于控制者的教育目的，不用于其他商业目的。控制者应持续告知父母，并转交父母查看或删除其子女数据的请求；处理者依据第8条予以办理。
4. **美国 — 删除和通知。** 许可协议终止时的删除适用第10条。如某州的学生隐私法就泄露通知或删除规定了更短的期限，处理者在控制者告知适用哪部法律后即予遵守。
