数据处理协议

https://scratcher.io/zh/data-processing-agreement

标准版本，最后更新于 2026 年 10 月 22 日。本数据处理协议是您在选用 Scratcher 时与 Scratcher ApS (CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø, Denmark) 拟定的协议的一部分。本协议的制定符合 GDPR 第 28 条的要求。

数据处理协议

本数据处理协议是客户与 Scratcher 所订立协议不可分割的一部分。如果本数据处理协议作为协议附件，则条款与条件中的第 10 条不适用，且应适用本数据处理协议。

1. 定义

1.1. 除非上下文另有明确要求，否则本数据处理协议中下列首字母大写的术语具有以下含义：

- “数据泄漏”是指导致所处理的个人数据遭到意外或无权的破坏、丢失、篡改或未经授权的披露（未经授权）或调阅的任何意外或无权的数据安全事件。
- “数据控制者”是指按 GDPR 定义确定个人数据处理目的和方式的客户。
- “数据处理者”是指受雇代表数据控制者处理个人数据的 Scratcher。
- “个人数据”是指数据处理者根据本协议代表数据控制者处理的与已识别或可识别的自然人相关的信息（GDPR 第 4 条第 1 款）。
- “GDPR”是指欧洲议会和理事会 2016 年 4 月 27 日关于在个人数据处理方面保护自然人及此类数据自由流动并废除第 95/46/EC 号指令的第 2016/679 号法规（通用数据保护条例）。
- “数据子处理者”是指除数据处理者的员工外，受数据处理者委托，根据其说明并在本数据处理协议指定的范围和目的内代表数据处理者处理个人数据的任何人员。

1.2. 除非上下文另有明确要求，否则上文未定义的首字母大写术语与协议中的定义具有相同含义。

2. 适用范围

2.1. 本数据处理协议中的条款和条件适用于数据处理者代表数据控制者并按照其指示处理个人数据的情形。

2.2. 当本数据处理协议中提及“数据处理者”时，数据处理协议的相关条款亦适用于数据处理者委托的任何数据子处理者。

3. 数据控制者指示与处理条件

3.1.

数据处理者应仅根据数据控制者的书面指示处理个人数据，包括将个人数据传输至第三国，除非数据处理者受适用的欧盟或成

员国法律要求必须这样做。在此情况下，数据处理者应在处理前将该法律要求告知数据控制者，除非该法律出于重大的公共利益禁止此类通知。

3.2.

数据处理者应处理数据控制者（包括其客户）在使用服务时上传或提交的那些数据主体类别的个人数据。代表数据控制者处理的个人数据类型和数据主体类别列于本数据处理协议的附录 A 中。

3.3.

双方同意将本数据处理协议以及数据控制者在使用服务时可能建立的协议视为数据控制者的书面指示。数据控制者可以通过调整服务的设置，向数据处理者提供有关收集个人数据的额外书面指示。双方还可以就执行数据控制者的其他指示及其价格达成书面协议。

3.4.

数据处理者应自数据控制者在使用服务时上传或传输个人数据时起开始处理个人数据，直至其被删除为止，但最长不超过本数据处理协议第 12 条规定的期限。

3.5. 如果数据处理者认为某项指示违反了 GDPR 或其他欧盟或成员国的数据保护规定，应立即通知数据控制者。

3.6. 数据控制者承诺，应数据处理者的要求，及时提供数据处理者代表数据控制者处理个人数据时全面符合 GDPR 所有要求所需的任何信息、文件或协助。

4. 个人数据的保密性

4.1.

数据处理者应仅将个人数据用于提供服务和行使其在本协议项下权利的目的。除非法律另有要求，数据处理者不得向第三方披露个人数据。

4.2.

数据处理者应确保仅向为其履行职责或向数据处理者提供服务而需要此类数据的员工或供应商授予个人数据的调阅权限，且所有获准处理个人数据的人员均已承诺保密或承担适当的法定保密义务。

4.3.

如果数据处理者为了符合法律要求而有义务向第三方（例如执法机关）披露个人数据，数据处理者应立即向数据控制者通知披露个人数据的要求，除非法律另有规定。

4.4. 这些保密义务在本数据处理协议终止后继续有效。

5. 技术和组织措施

5.1.

考虑到现有技术水平、实施成本以及处理的性质、范围、背景和目的，以及对自然人权利和自由造成不同概率和严重程度的风

险，数据处理者应在处理个人数据之前以及处理个人数据的任何时候，实施确保个人数据安全所需的适当技术和组织措施。在选择和实施技术和组织措施以确保适当的安全水平时，数据处理者应特别考虑到因处理数据主体的个人数据、因意外或无权破坏、丢失、篡改、未经授权的披露或无权调阅已传输、存储或以其他方式处理的数据而产生的风险。

5.2. 由于数据处理者是其领域的专业人员，并具备提供服务的知识和经验，数据处理者应选择并确定实现本数据处理协议第 5.1
条设定目标所需的技术和组织措施，但无论如何，此类措施应符合适用法律的要求。尽管如此，数据控制者仍有权就实施技术和组织安全措施向数据处理者提出指示和建议。数据处理者应考虑数据控制者的此类建议，并（i）向数据控制者提供合理的答复，说明数据处理者将如何实施数据控制者的指示；（ii）立即采取步骤实施此类措施。

5.3. 数据处理者在签署本数据处理协议时所实施的技术和组织措施描述于附录 C 中。数据处理者维护着一套通过 ISO/IEC 27001 认证的信息安全管理体系，并可能会随着时间的推移更新这些措施，前提是整体安全水平不会降低。

5.4. 考虑到处理的性质和现有的信息，数据处理者应协助数据控制者确保遵守 GDPR 第 32 条规定的义务。

6. 数据处理审计

6.1. 数据处理者应向数据控制者提供证明符合 GDPR 第 28 条所规定的义务所需的所有信息，包括其现行的 ISO/IEC 27001 证书，并应要求提供适用性声明（Statement of Applicability）。

6.2.
为核实数据处理者是否妥善处理个人数据，数据控制者有权在下列条件下对该等处理进行审查：（i）审计必须仅与个人数据的处理相关；（ii）数据控制者必须在合理的期限内通知数据处理者进行审计的意愿，该期限不得少于 4
周；（iii）审计的进行不得干扰数据处理者的日常活动；（iv）审计费用由数据控制者承担；（v）审计必须由独立的第三方人员进行，且该人员的候选资格必须事先获得数据处理者的批准（数据处理者不得无理拒绝批准），并且该人员必须承诺保护数据处理者的保密信息。

6.3.
数据处理者有权因协助开展审计而收取报酬。该报酬的数额由数据处理者结合其因审计产生的费用确定。数据处理者应在审计前将报酬数额告知数据控制者。

6.4. 由有管辖权的监管机构进行的审计和审查不受第 6.2 条和第 6.3 条条件的约束。

6.5.
如果数据控制者对审计结果不满意，数据控制者有权在诉讼外程序下单方面终止本数据处理协议和本协议。在此情况下，终止协议是数据控制者可以采取的唯一措施，且数据处理者没有义务向数据控制者赔偿任何损失。

7. 数据子处理者

7.1.

数据控制者在此授予数据处理者一般的事先同意，允许其委托数据子处理者在本数据处理协议指定的范围和目的内代表数据处理者处理个人数据。

7.2.

数据处理者应确保与受托的数据子处理者签订了书面协议，根据该协议，数据子处理者承诺遵守与本数据处理协议中规定的相同数据保护义务，特别是提供充分的保证以实施适当的技术和组织措施，从而使处理符合 GDPR 的要求。数据处理者应对数据子处理者履行义务向数据控制者承担责任。

7.3. 目前的数据子处理者名单列于本数据处理协议的附录 B 中。数据处理者应在计划变更或引入新数据子处理者前至少 14 个日历日将此类信息提供给数据控制者，从而将相关计划通知数据控制者。

7.4. 如果数据控制者在收到数据处理者根据本数据处理协议第 7.3 条规定的程序发出的通知后，继续使用服务，则应视为数据控制者已同意数据处理者的此类行为。如果数据控制者不同意此类变更或数据子处理者的引入，数据控制者有权通过诉讼外程序单方面终止本协议。在此情况下，终止本协议是数据控制者可以采取的唯一措施，且数据处理者没有义务赔偿数据控制者的任何损失。

7.5.

如果数据控制者撤回其委托数据子处理者的一般同意，数据处理者有权通过诉讼外程序单方面终止本协议，且此类终止应被视为因重要原因而作出，数据控制者应被视为未因该终止而遭受任何损失。

8. 数据泄漏

8.1. 数据处理者在获知影响个人数据的数据泄漏后，应在不延误的情况下（但最迟不得晚于获知数据泄漏后的 24 小时内），通过销售建议书（Sales Proposal）中指定的电子邮件地址通知数据控制者；若未指定，则通过数据控制者账户所有者的电子邮件地址通知。结合所提供服务的性质、个人数据的处理情况以及现有信息，数据处理者应向数据控制者提供以下信息：（i）数据泄漏的性质，包括在可能的情况下数据主体的类别和大致数量；（ii）数据泄漏可能导致的后果；（iii）数据处理者已实施或建议采取的应对数据泄漏的措施，包括在适当情况下减轻数据泄漏可能产生的负面后果的措施；（iv）数据保护官或任何其他可提供进一步信息的联系人的姓名和联系信息。

8.2. 数据处理者应记录所有数据泄漏，包括与数据泄漏事实相关的记录、其影响及采取的纠正措施。在 GDPR 或其他适用法律规定的情况下，数据处理者应向监管机构提供此类记录文件。

8.3. 考虑到处理的性质和现有的信息，数据处理者应协助数据控制者确保遵守 GDPR 第 33 条和第 34 条规定的义务。数据控制者仍负责通知监管机构并在需要时通知数据主体。除非数据泄漏是由数据处理者违反本数据处理协议项下的义务所致，否则除第 8.1 条中的通知外，数据处理者提供的额外协助可能会产生附加费用。

9. 个人数据向第三国的传输

9.1. 数据处理者将个人数据传输至第三国（欧盟/欧洲经济区以外）仅能基于数据控制者的书面指示进行，且应始终符合 GDPR 第 V 章的规定。

9.2. 数据控制者对附录 B 中所列数据子处理者的批准，即构成了对这些数据子处理者按照附录 B 所述进行数据传输的书面指示。每一次此类传输都应基于欧盟委员会的充分性认定（包括适用于已认证接收方的《欧盟-美国数据隐私框架》）、欧盟委员会的标准合同条款，或 GDPR 第 V 章规定的其他传输工具。

10. 合作

10.1. 结合所提供服务的性质、客户数据的处理情况以及现有信息，数据处理者应与数据控制者合作，确保履行 GDPR 第 32–36 条规定的义务。为此目的，且仅在本数据处理协议规定的范围内，数据处理者应向数据控制者提供妥善履行 GDPR 项下数据控制者义务所需的请求信息。

10.2.
如果处理类型（特别是使用新技术时）并考虑到处理的性质、范围、背景和目的，可能对自然人的权利和自由造成高风险，数据处理者应在处理前协助数据控制者开展拟定处理活动对个人数据保护的影响评估。

10.3.
如果数据主体、监管机构或第三方要求数据处理者根据法律提供有关所处理个人数据的任何信息，数据处理者应在不延误的情况下将此类请求转发给数据控制者。数据处理者承诺在必要的范围内协助数据控制者回应数据主体、监管机构或第三方的请求，并履行与实现数据主体权利相关的控制者义务，包括但不限于更正和删除个人数据的权利、个人数据可携权、反对和限制处理的权利。数据处理者应确保在法律规定的时限内传达其持有的信息。

11. 数据控制者义务

11.1.
数据控制者应全权自行决定并负责确定向数据处理者提供的个人数据类型和数据主体类别，并仅向数据处理者提供数据处理者妥善提供服务所必需的个人数据。数据控制者应承担所涉及的所有风险，包括数据处理者接收到超出必要范围的个人数据的风险。

11.2.
数据控制者声明并保证，其已取得并在本协议有效期内将持续维持向数据处理者提供个人数据以及委托数据处理者根据本协议处理个人数据所需的全部必要许可和授权。

12. 个人数据的删除与退回

12.1.
在本协议或本数据处理协议终止时，数据处理者应根据数据控制者的选择，删除代表数据控制者处理的所有个人数据，或将所有个人数据退还给数据控制者（数据控制者可以随时从服务中导出其数据）并删除任何现有副本，并向数据控制者出具已完成该操作的证明，除非欧盟或成员国法律要求保留个人数据。备份中的副本将随着备份在其正常周期内到期而被删除，在此期间

不会用于任何其他目的。

13. 责任

13.1.

无论数据控制者遭受何种损害，数据处理者在本数据处理协议项下的全部责任限制如下：数据处理者及其任何供应商对因本数据处理协议产生或与本数据处理协议相关的任何及所有索赔承担的累计责任总额，不得超过数据控制者在产生索赔事件发生之日前十二（12）个月内因服务实际向数据处理者支付的金额。在适用法律允许的最大范围内，在任何情况下，数据处理者或其供应商均不对任何特殊的、附带的、间接的或后果性的损害（包括但不限于利润损失、数据或其他信息丢失、业务中断、人身伤害、隐私丧失的损害）承担责任，即使数据处理者或供应商已被告知发生此类损害的可能性，且即使救济手段未达到其主要目的。

13.2. 第 13.1 条中的限制仅适用于双方之间。其不适用于根据适用法律不能予以限制的责任，亦不影响数据主体在 GDPR 第 82 条下的权利。

14. 有效期与终止

14.1.

本数据处理协议自本协议生效之日起生效，并在本协议保持有效的期间内持续有效。数据处理者的义务在其代表数据控制者处理个人数据的整个期间内持续有效。

15. 附则

15.1. 数据处理者应在拟议变更前至少 30

天发出任何对数据处理协议进行修改的通知。如果数据控制者在数据处理协议变更公布后继续使用服务，则应视为数据控制者同意数据处理协议的变更。如果数据控制者不同意变更，数据控制者将无法使用服务，并有权终止本协议。

15.2. 如果本数据处理协议与本协议之间存在冲突，就个人数据的处理而言，以本数据处理协议为准。

15.3. 本数据处理协议受与本协议相同的法律管辖，争议的解决方式与本协议相同。

15.4. 附录：

- 附录 A：个人数据处理详情；
- 附录 B：已批准的数据子处理者；
- 附录 C：技术和组织措施

附录 A – 个人数据处理详情

主体事项与期限	在协议有效期内与服务相关的个人数据处理，以及此后直到根据第 12 条删除或退回个人数据为止。
处理的性质	托管与存储；通过数据控制者的活动和表单收集个人数据；在服务中展示、导出和删除；向数据控制者设置的参与者发送电子邮件和消息（例如确认函、验证码和奖品通知）；根据数据控制者的指示通过集成、网络钩子（webhooks）和 API 传输至数据控制者自己的系统；支持与错误处理。
个人数据处理的目的	使数据控制者能够按照协议约定使用数据处理者的服务
个人数据处理操作	收集与存储客户数据，包括在使用服务期间提供的个人数据
个人数据类型	名、姓、电子邮件、IP 地址以及据此推导的大致位置、注册日期和时间（创建时间）以及其他数据（如生日和电话号码，若由客户收集）。根据数据控制者设置活动的方式，还包括活动问题的回答、游戏结果和所中奖品、验证码、同意记录、参与者上传的文件（例如图像）以及浏览器和设备信息等技术数据。
特殊数据类别	未设想。数据控制者不得通过服务收集特殊类别的个人数据（GDPR 第 9 条）或关于刑事判决的数据（GDPR 第 10 条），除非另有书面约定。
数据主体类别	数据控制者（客户）活动的参与者、未注册的数据控制者活动的访客（IP 地址、大致位置和浏览器信息），以及数据控制者的服务用户（在其数据代表数据控制者被处理的范围内）。
个人数据处理地点	个人数据应在数据处理者的场地以及位于欧盟的虚拟服务器上处理，并由附录 B 中所列的数据子处理者在其中所述的地点进行处理。
处理期限/存储期限	由数据控制者在服务中设置。根据条款和条件第 9.4 条，数据处理者可以删除超过三（3）年的个人数据。

附录 B – 已批准的数据子处理者

在签署本数据处理协议时，数据控制者批准委托下述数据子处理者。在接收方获得认证的情况下，向欧盟/欧洲经济区以外的传输基于《欧盟-美国数据隐私框架》，或基于欧盟委员会的标准合同条款（第 9.2 条）。

数据子处理者	处理说明	处理地点
Amazon Web Services EMEA SARL, Luxembourg (AWS)	服务的托管：服务器、数据库、文件存储、备份、缓存和日志	欧盟（瑞典斯德哥尔摩）。内容通过 Amazon CloudFront 网络交付，该网络可能会在欧盟/欧洲经济区以外的边缘节点处理流量。
ClickHouse, Inc. (ClickHouse Cloud)	用于活动统计分析的数据库（如访问量、参与度与注册数），包含 IP 地址和浏览器信息	欧盟（德国法兰克福），托管于 AWS。
Mailgun Technologies, Inc. (part of Sinch)	向参与者发送由数据控制者设置的电子邮件（如确认函、验证码和奖品通知），包括开启追踪时的传送、打开和点击记录	欧盟（消息数据的欧盟区域）；有限的账户信息可能会在全球范围内处理。
ip-api.com	查询参与者 IP 地址的大致位置并检测来自代理和数据中心的流量，以防止欺诈和机器人攻击	罗马尼亚（欧盟）；不能排除在欧盟/欧洲经济区以外进行处理或数据传输的可能性。
Google (Gemini API)	服务中的 AI 功能，例如 AI 助手、翻译和文本生成。参与者数据仅以假名化或聚合形式发送（例如首字母缩写、电子邮件域名和注册时间），除非数据控制者的用户自行输入该数据	美国以及可能的其他国家/地区，具体取决于 API 端点和处理配置。
Functional Software, Inc. (Sentry)	服务的错误监控和会话回放，用于查找和修复错误。报告可包含内部用户及账户 ID 以及关于数据控制者用户的浏览器的技术数据。会话回放中的文本已进行遮罩处理	欧盟（德国，Sentry 欧盟区域）。
Cloudflare, Inc. (Turnstile)	活动表单上的机器人防护，仅当数据控制者为某个活动开启时有效。接收参与者的 IP 地址和浏览器信号	全球网络；处理可能会在欧盟/欧洲经济区以外发生。
Features & Labels, Inc. (fal.ai)	服务中的 AI 图像生成与编辑、背景消除和配音功能。接收数据控制者用户提交的提示词和图像	美国。
Adressevælger (adressevaelger.dk)	活动表单中的地址建议，仅当数据控制者为某个活动开启时有效。接收参与者输入的地址文本和参与者的 IP 地址	丹麦（欧盟）。

附录 C – 技术和组织措施

数据处理者维护着一套由必维国际检验集团（Bureau Veritas，证书编号 FIHSK27150F）认证的符合 ISO/IEC 27001:2022 的信息安全管理体系。相关措施包括：

- **托管与物理安全：**所有客户数据均存储在位于欧盟的 Amazon Web Services (AWS) 数据中心。数据处理者不运行自己的服务器；物理与环境安全由通过 ISO 27001 和 SOC 2 认证的 AWS 提供。
- **网络安全：**服务器和数据库运行在无法从互联网直接访问的私有网络（Amazon VPC）中。仅负载均衡器和内容分发网络对外公开，并受到 Web 应用防火墙（AWS WAF）和 DDoS 防护的保护。
- **加密：**所有流量均使用 TLS (HTTPS) 加密。数据库、文件和备份在静止状态下均采用 AES-256 加密。集成凭据在应用层进行了附加加密。密码采用 bcrypt 进行哈希和加盐处理。
- **访问控制：**为客户用户提供基于角色的访问控制、双因子身份验证和 Google 单点登录、会话超时以及限制登录尝试频率。员工访问遵循最小权限和按需知晓原则，尽可能使用独立账户和多因子身份验证，每年至少审查一次，并在离职时撤销访问权限。
- **隔离：**客户数据按账户进行逻辑隔离（租户隔离），且每个请求均经过授权。
- **日志记录与监控：**对基础设施的更改均记录在防篡改的审计追踪中，应用程序日志集中收集，平台得到全天候监控，客户可以在活动日志中查看其用户的活动情况。
- **可用性与韧性：**每日进行加密备份并保存至少 7 天且与生产环境分开存储，每年至少测试一次恢复，业务连续性和灾难恢复计划每年都会进行审查和演练。
- **事件管理：**拥有成文的流程来报告、评估、控制、分析和跟踪安全事件，包括根据第 8 条通知数据泄漏事件。
- **安全开发与运维：**服务器作为无 SSH 访问权限的不可变容器运行，绝不手动更改，且更改在发布前均经过测试。
- **人员：**员工受保密协议约束，并作为信息安全管理体系的一部分接受信息安全意识培训。有权访问基础设施的合作伙伴本身也通过了 ISO 27001 认证，且仅获得其工作所需的访问权限。
- **数据最小化与删除工具：**数据控制者决定每个活动收集哪些数据，并可以导出、删除或自动删除参与者数据。