Data Processing Agreement

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

Standard version, last updated 22 October 2026. This Data Processing Agreement forms part of the agreement between you and Scratcher ApS (CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø, Denmark) when you use Scratcher. It is drafted to meet the requirements of Article 28 of the GDPR.

Data Processing Agreement

This Data Processing Agreement is an integral part of the Agreement between the Customer and Scratcher. If this Data Processing Agreement is attached to the Agreement, clause 10 of the Terms and Conditions shall not apply and this Data Processing Agreement shall apply.

1. Definitions

1.1. Unless the context expressly requires otherwise, the following capitalised terms in this Data Processing Agreement shall have the following meanings:

- “Data Breach” is any accidental or unlawful breach of personal data security resulting in accidental or unlawful destruction, loss, alteration or unauthorised disclosure (without authorisation) of or access to the processed Personal Data.
- “Data Controller” means the Customer when it determines the purposes and means of the processing of Personal Data as defined in the GDPR.
- “Data Processor” means the Scratcher when it is engaged in processing Personal Data on behalf of the Data Controller.
- “Personal Data” means any information relating to an identified or identifiable natural person (Article 4(1) GDPR) that the Data Processor processes on behalf of the Data Controller under the Agreement.
- “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- “Sub-Processor” means any person, except an employee of the Data Processor, engaged by the Data Processor for the processing of the Personal Data on behalf of the Data Processor and in accordance with its instructions to the extent and for the purposes specified in the Data Processing Agreement.

1.2. Capitalised terms not defined above shall have the same meaning as defined in the Agreement unless the context expressly requires otherwise.

2. Scope

2.1. The terms and conditions contained in this Data Processing Agreement apply to the processing of Personal Data by the Data Processor on behalf of and under the instructions of the Data Controller.

2.2. Where the Data Processor is referred to in this Data Processing Agreement, the relevant provisions of the Data Processing Agreement shall also apply to any Sub-Processor engaged by the Data Processor.

3. Data Controller Instructions and Processing Conditions

3.1. The Data Processor shall process the Personal Data only in accordance with the documented instructions of the Data Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2. The Data Processor shall process the Personal Data of those categories of data subjects that the Data Controller (including its customers) uploads or submits when using the Services. The types of Personal Data and categories of data subjects processed on behalf of the Data Controller are listed in Appendix A to this Data Processing Agreement.

3.3. The Parties agree to consider this Data Processing Agreement and the Agreement that may be established by the Data Controller when using the Services as the documented instructions of the Data Controller. The Data Controller may provide the Data Processor with additional documented instructions for the collection of personal data by adjusting the settings of the Services. The Parties may also agree in writing on the execution of additional instructions of the Data Controller and the price thereof.

3.4. The Data Processor shall process the Personal Data from the moment it is uploaded or transmitted by the Data Controller when using the Services until it is removed, but no longer than the period specified in Article 12 of this Data Processing Agreement.

3.5. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

3.6. The Data Controller undertakes, at the Data Processor's request, to provide without delay any information, documents or assistance necessary for the Data Processor to properly comply with all the requirements of the GDPR when processing the Personal Data on behalf of the Data Controller.

4. Confidentiality of the Personal Data

4.1. The Data Processor shall use the Personal Data only for the purpose of providing the Services and exercising its rights under the Agreement. Unless otherwise required by law, the Data Processor shall not disclose the Personal Data to third parties.

4.2. The Data Processor shall ensure that access to the Personal Data is granted only to those employees or suppliers of the Data Processor who require such data for the performance of their duties or for the provision of services to the Data Processor, and that all persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3. If the Data Processor is obliged to disclose the Personal Data to third parties (e.g. law enforcement authorities) in order to comply with the requirements of the law, the Data Processor shall immediately inform the Data Controller of the requirements to disclose the Personal Data, unless otherwise required by the law.

4.4. These confidentiality obligations shall survive the termination of this Data Processing Agreement.

5. Technical and Organisational Measures

5.1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying probability and severity for the rights and freedoms of natural persons, the Data Processor shall implement, before the processing of Personal Data and at any time during the processing of Personal Data, appropriate technical and organisational measures necessary to ensure the security of the Personal Data. In selecting and implementing technical and organisational measures to ensure an adequate level of security, the Data Processor shall in particular take into account the risks arising from the processing of the data subject's Personal Data, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or unlawful access to the data transmitted, stored or otherwise processed.

5.2. As the Data Processor is a professional in its field and has knowledge and experience in the provision of the Services, the Data Processor shall select and determine the technical and organisational measures necessary to achieve the objectives set out in clause 5.1 of this Data Processing Agreement, but such measures shall, in any case, comply with the requirements of the applicable laws. Nevertheless, the Data Controller shall have the right to give instructions and suggestions to the Data Processor regarding the application of technical and organisational security measures. The Data Processor shall take into account such suggestions from the Data Controller, consider them and (i) provide the Data Controller with a reasoned response as to how the Data Processor will implement the instructions of the Data Controller (ii) take immediate steps to implement such measures.

5.3. The technical and organisational measures implemented by the Data Processor at the time of entering into this Data Processing Agreement are described in Appendix C. The Data Processor maintains an information security management system certified to ISO/IEC 27001 and may update the measures over time, provided that the overall level of security is not reduced.

5.4. Taking into account the nature of the processing and the information available to it, the Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Article 32 of the GDPR.

6. Data Processing Audit

6.1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR, including its current ISO/IEC 27001 certificate and, on request, its Statement of Applicability.

6.2. In order to verify whether the Data Processor is properly processing the Personal Data, the Data Controller shall have the right to conduct inspections of such processing under the following conditions: (i) the audit must relate only to the processing of the Personal Data; (ii) the Data Controller must notify the Data Processor of the wish to conduct an audit within a reasonable time period, which shall not be less than 4 weeks; (iii) the audit must be conducted in such a way that it does not interfere with the daily activities of the Data Processor; (iv) the audit must be conducted at the expense of the Data Controller; (v) the audit must be conducted by an independent person whose candidature must be approved in advance by the Data Processor, such approval not to be unreasonably withheld, and who must undertake to protect the Confidential Information of the Data Processor.

6.3. The Data Processor shall be entitled to receive remuneration for its assistance in carrying out the audit. The amount of such remuneration shall be determined by the Data Processor taking into account the costs incurred by the Data Processor in connection with the audit. The Data Processor shall inform the Data Controller of the amount of the remuneration prior to the audit.

6.4. Audits and inspections carried out by a competent supervisory authority are not subject to the conditions in clauses 6.2 and 6.3.

6.5. If the Data Controller is not satisfied with the results of the audit, the Data Controller shall have the right to unilaterally, under the out-of-court procedure, terminate this Data Processing Agreement and the Agreement. In this case, the termination of the Agreements shall be the only measure that may be taken by the Data Controller and the Data Processor shall not be obliged to compensate any damages to the Data Controller.

7. Sub-Processors

7.1. The Data Controller hereby grants the Data Processor general prior consent to engage the Sub-Processors who will process the Personal Data on behalf of the Data Processor within the scope and for the purposes specified in this Data Processing Agreement.

7.2. The Data Processor shall ensure that a written agreement has been concluded with the Sub-Processors engaged, under which the Sub-Processors undertake to comply with the same data protection obligations as those set out in this Data Processing Agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. The Data Processor shall be liable to the Data Controller for the performance of the obligations of the Sub-Processors.

7.3. The current list of Sub-Processors shall be indicated in Appendix B of this Data Processing Agreement. The Data Processor shall notify the Data Controller about its plans to replace or engage a new Sub-Processor by making such information available to the Data Controller no later than 14 calendar days prior to the planned event.

7.4. If the Data Controller continues to use the Services following the replacement or engagement of a new Sub-Processor after being notified by the Data Processor in accordance with the procedure set out in clause 7.3 of this Data Processing Agreement, it shall be deemed that the Data Controller has consented to such actions by the Data Processor. If the Data Controller does not agree with such replacement or involvement of the Sub-Processor, the Data Controller shall have the right to terminate the Agreement unilaterally by means of an out-of-court procedure. In such case, termination of the Agreement shall be the only measure that may be taken by the Data Controller and the Data Processor shall not be obliged to compensate the Data Controller for any damages.

7.5. If the Data Controller withdraws its general consent to engage the Sub-Processor, the Data Processor shall have the right to unilaterally terminate the Agreement through an out-of-court procedure, and such termination shall be deemed to have been made for important reasons, and the Data Controller shall be deemed not to have suffered any damage as a result of such termination.

8. Data Breach

8.1. The Data Processor shall notify the Data Controller of any Data Breach affecting the Personal Data, by the email address stated in the Sales Proposal or, if none is stated, the email address of the owner of the Data Controller's account, without undue delay but no later than within 24 hours after becoming aware about the Data Breach, and taking into consideration the nature of the provided Services and processing of the Personal Data and available information, shall provide the following information to the Data Controller: (i) the nature of the Data Breach, including, where possible, the categories of the data subjects and approximate number thereof; (ii) possible consequences of the Data Breach; (iii) measures implemented by the Data Processor or proposed to be taken to address the Data Breach, including, where appropriate, measures for mitigating possible negative consequences of the Data Breach; (iv) full name and contact information of data protection officer or any other contact person that could provide further information.

8.2. The Data Processor shall document all the Data Breaches, including the facts relating to the Data Breach, its impact and the corrective measures taken. In cases provided for by the GDPR or other applicable legislation, the Data Processor shall provide such documentation to the supervisory authority.

8.3. Taking into account the nature of the processing and the information available to it, the Data Processor shall assist the Data Controller in ensuring compliance with its obligations under Articles 33 and 34 of the GDPR. The Data Controller remains responsible for notifying the supervisory authority and, where required, the data subjects. Except where a Data Breach is caused by a breach of the Data Processor's obligations under this Data Processing Agreement, the Data Processor's assistance beyond the notification in clause 8.1 may be subject to additional charges.

9. Transfer of the Personal Data to Third Countries

9.1. Any transfer of personal data to third countries (outside the EU/EEA) by the Data Processor shall only take place on the basis of documented instructions from the Data Controller and shall always be in compliance with Chapter V of the GDPR.

9.2. The Data Controller's approval of the Sub-Processors listed in Appendix B constitutes a documented instruction for the transfers that those Sub-Processors make, as described there. Each such transfer shall be based on an adequacy decision of the European Commission (including the EU–US Data Privacy Framework for certified recipients), the European Commission's Standard Contractual Clauses or another transfer tool under Chapter V of the GDPR.

10. Cooperation

10.1. Taking into consideration the nature of the Services provided and the processing of the Customer Data and available information, the Data Processor shall cooperate with the Data Controller to ensure the performance of the obligations specified in Articles 32–36 of the GDPR. For this purpose, and only to the extent specified in this Data Processing Agreement, the Data Processor shall provide the Data Controller with the requested information necessary for the proper performance of the Data Controller's obligations under the GDPR.

10.2. Where the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Data Processor shall, prior to the processing, provide support to the Data Controller in carrying out an assessment of the impact of the envisaged processing operations on the protection of Personal Data.

10.3. Should the data subject, the supervisory authority or a third party request the Data Processor to provide any information about the processed Personal Data pursuant to the laws, the Data Processor shall forward such requests to the Data Controller without undue delay. The Data Processor undertakes to assist the Data Controller to the extent necessary in responding to the requests of data subjects, supervisory authorities or third parties and in fulfilling the Data Controller's obligations relating to the implementation of the rights of data subjects, including but not limited to the right to rectification and erasure of personal data, the right to portability of personal data, the right to object to and restrict the processing. The Data Processor shall ensure that the information in its possession is communicated within the time limits established by law.

11. Data Controller Obligations

11.1. The Data Controller shall determine, at its sole discretion and responsibility, the types of Personal Data and categories of data subjects to be provided to the Data Processor and shall provide to the Data Processor only the Personal Data necessary for the proper provision of the Services by the Data Processor. The Data Controller shall bear all the risks involved, including the risks of the Data Processor receiving more Personal Data than necessary.

11.2. The Data Controller represents and warrants that it has obtained and will maintain throughout the term of the Agreement all necessary permits and authorisations required to provide the Personal Data to the Data Processor and to engage the Data Processor to process the Personal Data under the Agreement.

12. Erasure and Return of Personal Data

12.1. Upon termination of the Agreement or this Data Processing Agreement, the Data Processor shall, at the choice of the Data Controller, delete all Personal Data processed on behalf of the Data Controller, or return all Personal Data to the Data Controller (the Data Controller can export its data from the Services at any time) and delete any existing copies, and certify to the Data Controller that it has done so, unless Union or Member State law requires the retention of the Personal Data. Copies in backups are deleted as the backups expire in their normal cycle and are not used for any other purpose in the meantime.

13. Liability

13.1. Irrespective of any damages suffered by the Data Controller, the entire Data Processor's liability under this Data Processing Agreement shall be limited as follows: the total liability of the Data Processor and any of its suppliers for any and all claims arising under or in connection with this Data Processing Agreement shall not exceed the amount actually paid by the Data Controller to the Data Processor for the Services during the twelve (12) months preceding the date of the event giving rise to the claim. To the maximum extent permitted by applicable law, in no event shall the Data Processor or its suppliers be liable for any special, incidental, indirect, or consequential damages (including, but not limited to, damages for loss of profits, data, or other information, business interruption, personal injury, loss of privacy), even if the Data Processor or a

supplier has been advised of the possibility of such damages and even if the remedy fails of its essential purpose.

13.2. The limitations in clause 13.1 apply between the parties only. They do not apply to liability that cannot be limited under applicable law and do not affect the rights of data subjects under Article 82 of the GDPR.

14. Validity and Termination

14.1. This Data Processing Agreement shall enter into force upon the entry into force of the Agreement and shall remain in force as long as the Agreement remains in force. The obligations of the Data Processor continue for as long as it processes Personal Data on behalf of the Data Controller.

15. Final Provisions

15.1. The Data Processor shall give notice of any intended change to the Data Processing Agreement at least 30 days prior to the intended change. If the Data Controller continues to use the Services after the announcement of changes to the Data Processing Agreement, it shall be deemed that the Data Controller agrees to the changes to the Data Processing Agreement. If the Data Controller does not agree to the changes, the Data Controller will not be able to use the Services and will have the right to terminate the Agreement.

15.2. In case of conflict between this Data Processing Agreement and the Agreement, this Data Processing Agreement prevails as regards the processing of Personal Data.

15.3. This Data Processing Agreement is governed by the same law, and disputes are settled in the same way, as set out in the Agreement.

15.4. Appendixes:

- Appendix A: Details of Processing of the Personal Data;
- Appendix B: Approved Sub-Processors;
- Appendix C: Technical and Organisational Measures

Appendix A – Details of the processing of Personal Data

Subject matter and duration	The processing of Personal Data in connection with the Services for the term of the Agreement, and afterwards until the Personal Data is deleted or returned under clause 12.
Nature of the processing	Hosting and storage; collection of Personal Data through the Data Controller's campaigns and forms; display, export and deletion in the Services; sending of emails and messages to participants that the Data Controller sets up (for example confirmations, codes and prize notifications); transfer to the Data Controller's own systems through integrations, webhooks and the API on the Data Controller's instruction; support and error handling.
Purpose of Personal Data Processing	To enable the Data Controller to use the Data Processor’s Services as agreed in the Agreement

Personal Data Processing operation	Collection and storage of the Customer Data including Personal Data provided while using the Services
Types of Personal Data	First name, last name, email, IP address and approximate location derived from it, the date and time of the registration (created at) and additional data such as birthday and phone number (if collected by the Customer). Depending on how the Data Controller sets up its campaigns, also answers to campaign questions, game results and prizes won, codes, consent records, files uploaded by participants (for example images) and technical data such as browser and device information.
Special categories of data	Not intended. The Data Controller shall not collect special categories of personal data (Article 9 GDPR) or data about criminal convictions (Article 10 GDPR) through the Services unless agreed in writing.
Categories of data subjects	The participants of the Data Controller (Customer) campaigns, visitors to the Data Controller's campaigns who do not sign up (IP address, approximate location and browser information), and the Data Controller's users of the Services to the extent their data is processed on behalf of the Data Controller.
Place of the Personal Data processing	Personal Data shall be processed on the premises of the Data Processor and on virtual servers located in the European Union, and by the Sub-Processors listed in Appendix B at the locations stated there.
Duration of the processing/Storage period	As set by the Data Controller in the Services. In line with clause 9.4 of the Terms and Conditions, the Data Processor may delete Personal Data that is older than three (3) years.

Appendix B – Approved Sub-Processors

At the time of entering into the Data Processing Agreement, the Data Controller approves the engagement of the Sub-Processors listed below. Transfers outside the EU/EEA are based on the EU–US Data Privacy Framework where the recipient is certified, or on the European Commission's Standard Contractual Clauses (clause 9.2).

Sub-Processor	Description of processing	Location of processing
Amazon Web Services EMEA SARL, Luxembourg (AWS)	Hosting of the Services: servers, databases, file storage, backups, caching and logs	European Union (Stockholm, Sweden). Content is delivered through the Amazon CloudFront network, which may handle traffic at edge locations outside the EU/EEA.
ClickHouse, Inc. (ClickHouse Cloud)	Analytics database for campaign statistics, such as visits, participations and sign-ups, including IP address and browser information	European Union (Frankfurt, Germany), hosted on AWS.

Sub-Processor	Description of processing	Location of processing
Mailgun Technologies, Inc. (part of Sinch)	Sending emails that the Data Controller sets up to participants, such as confirmations, codes and prize notifications, including delivery, opens and clicks when tracking is enabled	European Union (EU region for message data); limited account information may be processed globally.
ip-api.com	Looking up the approximate location of participants' IP addresses and detecting traffic from proxies and data centres, to stop fraud and bots	Romania (EU); processing or data transfers outside the EU/EEA cannot be ruled out.
Google (Gemini API)	AI features in the Services, such as the AI assistant, translations and text generation. Participant data is only sent in pseudonymised or aggregated form (for example initials, email domain and time of sign-up), unless the Data Controller's users enter it themselves	United States and potentially other countries, depending on the API endpoint and processing configuration.
Functional Software, Inc. (Sentry)	Error monitoring and session replays for the Services, to find and fix errors. Reports can include internal user and account IDs and technical data about the browser of the Data Controller's users. Text in session replays is masked	European Union (Germany, Sentry EU region).
Cloudflare, Inc. (Turnstile)	Bot protection on campaign forms, only when the Data Controller turns it on for a campaign. Receives the participant's IP address and browser signals	Global network; processing may occur outside the EU/EEA.
Features & Labels, Inc. (fal.ai)	AI image generation and editing, background removal and voice-overs in the Services. Receives the prompts and images that the Data Controller's users submit	United States.
Adressevælger (adressevaelger.dk)	Address suggestions in campaign forms, only when the Data Controller turns it on for a campaign. Receives the address text the participant types and the participant's IP address	Denmark (EU).

Appendix C – Technical and Organisational Measures

The Data Processor maintains an information security management system certified to ISO/IEC 27001:2022 by Bureau Veritas (certificate no. FIHSK27150F). The measures include:

- **Hosting and physical security:** all customer data is stored in Amazon Web Services (AWS) data centres in the European Union. The Data Processor does not run its own servers; physical and environmental security is provided by AWS, which is certified to ISO 27001 and SOC 2.
- **Network security:** servers and databases run in a private network (Amazon VPC) that cannot be reached from the internet. Only the load balancers and the content delivery network are public, protected by a

web application firewall (AWS WAF) and DDoS protection.

- **Encryption:** all traffic is encrypted with TLS (HTTPS). Databases, files and backups are encrypted at rest with AES-256. Credentials for integrations are additionally encrypted at application level. Passwords are hashed and salted with bcrypt.
- **Access control:** role-based access control for customer users, two-factor authentication and Google single sign-on, session timeouts and rate-limited login attempts. Employees' access follows least privilege and need-to-know, uses unique accounts and multi-factor authentication where possible, is reviewed at least once a year and is revoked when someone leaves.
- **Separation:** customer data is logically separated by account (tenant isolation), and every request is authorised.
- **Logging and monitoring:** changes to the infrastructure are recorded in a tamper-evident audit trail, application logs are collected centrally, the platform is monitored around the clock, and customers can see their users' activity in an activity log.
- **Availability and resilience:** daily encrypted backups kept for at least seven days and stored separately from production, restores tested at least once a year, and business continuity and disaster recovery plans that are reviewed and exercised every year.
- **Incident management:** a documented process to report, assess, contain, analyse and follow up on security incidents, including notification of Data Breaches under clause 8.
- **Secure development and operations:** servers run as immutable containers without SSH access that are never changed by hand, and changes are tested before release.
- **People:** employees are bound by confidentiality and receive information security awareness training as part of the information security management system. Partners with access to the infrastructure are themselves ISO 27001 certified and only receive the access their work requires.
- **Data minimisation and deletion tools:** the Data Controller decides which data each campaign collects, and can export, delete or automatically delete participant data.