

Appendix 1: Data Processing Agreement

Effective from: 1 October 2026 · Version 1.0

This Data Processing Agreement ("**DPA**") sets out the data protection obligations and rights of the parties when Artur Mkrtchyan Ventures UG (haftungsbeschränkt), Pettenkoferstraße 9a, 10247 Berlin, Germany, registered with the Amtsgericht Charlottenburg under HRB 222561 B, represented by its managing director, Artur Mkrtchyan ("**AllBack**" or "**Contractor**"), processes personal data on behalf of the customer ("**Customer**") under the Terms and Conditions for the Use of AllBack ("**Main Agreement**").

This DPA is part of the Main Agreement. It applies when the Customer accepts the Main Agreement, without a separate signature. A Customer that needs a signed copy can ask for one at hello@allback.ai.

1. Scope of application

1.1 When AllBack provides the services under the Main Agreement, it processes personal data that the Customer makes available, or that people give in the Customer's forms, for the purpose of providing the services ("**Customer Data**"). The Customer is the controller of the Customer Data within the meaning of Art. 4 No. 7 GDPR, and AllBack is its processor within the meaning of Art. 4 No. 8 GDPR.

1.2 In the event of contradictions between this DPA and other agreements between the parties, in particular the Main Agreement, the provisions of this DPA prevail.

2. Subject-matter and scope of the processing, and the Customer's instructions

2.1 AllBack processes the Customer Data only on behalf of the Customer and in accordance with the Customer's documented instructions, unless the law of the European Union or a Member State requires AllBack to process it. In such a case, AllBack informs the Customer of that legal requirement before the processing, unless that law prohibits such information on important grounds of public interest.

2.2 AllBack processes the Customer Data only in the nature, to the extent, and for the purpose described in Annex 1. The processing concerns only the types of personal data and the categories of data subjects described in Annex 1.

2.3 The duration of the processing corresponds to the term of the Main Agreement, and to the periods for deletion in Section 8. The Customer may terminate this DPA and the Main Agreement if AllBack violates obligations under this DPA or instructions of the Customer, and does not remedy the violation without delay after a warning from the Customer. In the event of a material breach, the Customer may terminate this DPA and the Main Agreement without notice and without a prior warning.

2.4 AllBack stores the database and the uploaded files with the Customer Data in the European Union. AllBack and its sub-processors may process Customer Data outside the European Economic Area ("EEA") only if the requirements of Articles 44 to 49 GDPR are met. Annex 3 names the sub-processors that process data outside the EEA, and the transfer mechanism for each.

2.5 The Main Agreement, and the settings that the Customer chooses on the Platform (for example the questions of a form, the people it is sent to, and the reminder plan), are the Customer's instructions. The Customer can give further instructions on the nature, scope, purposes, and means of the processing. The Customer confirms oral instructions in writing or by email.

2.6 If the Customer gives instructions that go beyond the services agreed in the Main Agreement and this DPA, the Customer bears the costs of carrying them out. Before AllBack carries out such instructions, it informs the Customer of the expected costs and waits for the Customer's confirmation. This does not apply to instructions to stop the processing as a whole, to delete some or all Customer Data, or to hand it over to the Customer.

2.7 If AllBack thinks that an instruction of the Customer violates this DPA, the GDPR, or other data protection law of the European Union or the Member States, it informs the Customer without delay in writing or text form. AllBack may suspend the instruction until the Customer confirms it in writing or text form. If the Customer insists on the instruction despite AllBack's concerns, the Customer indemnifies AllBack against all damages and costs that AllBack incurs as a result of carrying it out.

3. Personnel

3.1 AllBack obliges all persons who process Customer Data to keep it confidential, unless they are subject to an appropriate statutory obligation of confidentiality.

3.2 AllBack ensures that all persons under its authority who have access to Customer Data process it only in accordance with this DPA and the Customer's instructions, unless the law of the European Union or a Member State requires them to process it.

4. Security of processing

4.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of the processing, as far as they are known to AllBack, and the risks of varying likelihood and severity for the rights and freedoms of the data subjects, AllBack implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

4.2 AllBack implements in particular the technical and organisational measures in Annex 2, and maintains them for the duration of the Main Agreement.

4.3 The Customer checks whether the measures in Annex 2 are also sufficient for circumstances of the processing that AllBack does not know, for example special categories of personal data that the Customer chooses to collect in its forms.

4.4 The technical and organisational measures are subject to technical progress. AllBack may replace them with other adequate measures, as long as the level of security does not fall below the level of the measures in Annex 2. AllBack informs the Customer in advance of significant changes.

If a change lowers the level of security so that it is no longer adequate, the Customer may terminate the Main Agreement and this DPA at the time when the change takes effect.

5. Sub-processors

5.1 AllBack uses the sub-processors in Annex 3 to process Customer Data. The Customer authorises them with the conclusion of this DPA.

5.2 AllBack may use further sub-processors under these conditions: AllBack informs the Customer before it uses a further sub-processor, by email or with a notice on its website. If the Customer does not object within fourteen (14) days after this information, the use of the further sub-processor counts as authorised.

5.3 If the Customer objects to a further sub-processor without good cause, AllBack may, at its own discretion, continue to provide the services without that sub-processor, or terminate the Main Agreement and this DPA in accordance with the Main Agreement.

5.4 AllBack obliges each sub-processor, by a written agreement, to the same data protection obligations as AllBack has towards the Customer under this DPA.

5.5 AllBack selects only sub-processors that give sufficient guarantees that they implement appropriate technical and organisational measures, so that the processing meets the requirements of the GDPR and this DPA.

5.6 If a sub-processor processes Customer Data outside the European Union or the EEA, and the conditions of Articles 44 to 48 GDPR are not met in another way, AllBack ensures that the data protection obligations are met by the EU Standard Contractual Clauses of 2021, Module Three (transfer from processor to processor), or by a certification under the EU-US Data Privacy Framework.

6. Rights of data subjects

6.1 AllBack takes all reasonable technical and organisational measures to assist the Customer in fulfilling its obligation to respond to requests from data subjects who exercise their rights.

6.2 In particular, and as far as it can, AllBack:

- informs the Customer if a data subject contacts AllBack directly with a request about Customer Data;
- gives the Customer all information in its possession about the processing of Customer Data that the Customer needs to respond to the request, and that the Customer does not have itself;
- corrects, deletes, or restricts the processing of Customer Data without delay on the Customer's instruction, as far as this is technically and reasonably possible; and
- ensures that the Customer can receive the Customer Data in a structured, commonly used, and machine-readable format, for example a CSV export of the answers, where the data subject has a right to data portability.

7. Other assistance to the Customer

7.1 AllBack notifies the Customer without undue delay after it becomes aware of a personal data breach that concerns Customer Data, in particular incidents that lead to the destruction, loss, alteration, or unauthorised disclosure of, or access to, Customer Data.

7.2 In the event of such a breach, AllBack takes, without delay, all necessary and reasonable measures to remedy it and, where necessary, to mitigate its possible adverse effects.

7.3 If the Customer must give information to an authority or a third party about the processing of Customer Data, or cooperate with them in another way, AllBack assists the Customer as far as it can. In particular, it gives all information and documents about the technical and organisational measures within the meaning of Art. 32 GDPR, the technical procedures of the processing, the places where Customer Data is processed, and the persons involved.

7.4 AllBack assists the Customer in complying with its obligations under Art. 32 GDPR, as far as AllBack can, considering the information that it has about the Customer's use of the services.

7.5 If the Customer must notify the supervisory authority or the data subjects under Art. 33 or 34 GDPR, AllBack assists the Customer on request, as far as it can. AllBack documents every personal data breach that concerns Customer Data, with the related facts, so that the Customer can prove that it met its reporting obligations.

7.6 AllBack supports the Customer with the information available to it, and assists within reason in a data protection impact assessment of the Customer, and in a later consultation of the supervisory authority under Art. 35 and 36 GDPR.

7.7 On request, AllBack gives the Customer the parts of its record of processing activities under Art. 30 para. 2 GDPR that concern the Customer Data.

8. Deletion and return of Customer Data

8.1 During the term of the Main Agreement, the Customer can export its answers and files at any time, and delete forms, requests, answers, and its account on the Platform.

8.2 When the Main Agreement ends, AllBack deletes all Customer Data at the end of the Grace Period of the Main Agreement, or returns it to the Customer on the Customer's instruction and then deletes the remaining copies, unless the law of the European Union or a Member State requires AllBack to keep it.

8.3 AllBack may keep backup copies of Customer Data for up to thirty (30) days after the deletion, or longer where the law requires it, as long as this DPA and Art. 32 GDPR continue to apply to them. Data in backups is deleted with the regular backup cycle.

8.4 AllBack keeps documentation that proves the proper processing of Customer Data for the statutory retention periods, also after the end of this DPA.

9. Evidence and inspections

9.1 AllBack regularly checks that it processes the Customer Data in accordance with this DPA, the scope in Annex 1, and the Customer's instructions.

9.2 AllBack documents how it meets its obligations under this DPA in a suitable manner, and gives the Customer, on request, the evidence that it needs to verify that AllBack complies with the GDPR and this DPA.

9.3 The Customer may audit AllBack once per year, or more often if a supervisory authority requires it or after a confirmed personal data breach. Audits take place during regular business hours, with at least four (4) weeks' prior notice in writing. Instead of an on-site audit, AllBack may give recent audit reports or certifications of independent third parties, and the Customer accepts them, unless it has reasonable doubts about AllBack's compliance. Audits must not obstruct AllBack's normal business more than necessary. The Customer bears the reasonable costs of an audit. AllBack may decline an auditor for good cause, and may require every auditor to sign a confidentiality agreement before the audit.

9.4 Under the GDPR, the Customer and AllBack are subject to the supervision of the competent supervisory authority. At the Customer's request, AllBack gives the supervisory authority the information it needs, and allows it, or persons it appoints, to carry out audits and inspections at AllBack.

10. Liability

Each party is liable only for damages that result from a breach of its own obligations under this DPA and the GDPR. Any further liability follows the liability provisions of the Main Agreement, except where mandatory statutory liability applies, in particular Art. 82 GDPR.

11. Miscellaneous

11.1 Amendments and side agreements to this DPA must be made in text form (email is sufficient).

11.2 The choice of law and the place of jurisdiction of the Main Agreement apply to this DPA too.

Annex 1: Description of the processing

Subject-matter. AllBack provides a service that collects information and files from many people for the Customer. The Customer, or an AI app that the Customer connects, creates forms. AllBack sends each person a personal link by email, prefilled with data that the Customer provides, reminds the people who have not answered, stores the answers and the uploaded files, and shows the Customer the status, insights, and exports. A form can also have one open link that anyone can use.

Nature of the processing. Collecting, recording, organising, storing, reading, using (in particular sending emails), disclosing by transmission to the Customer and to the people the Customer authorises, restricting, and erasing.

Purpose. The performance of the Main Agreement: to collect the information that the Customer asks for, to remind the people who have not answered, and to give the answers to the Customer.

Types of personal data.

- Contact data of the people the Customer asks: name and email address.

- Data that the Customer adds to prefill a form, for example a company name or a job title. The Customer decides which data this is.
- Answers, uploaded files, and signatures that people give in the Customer's forms. The Customer decides which questions a form asks.
- Event data of a form: when a person opened a link, started, read a document, and sent the answers, and how many reminders the person got.
- Email data: the emails that AllBack sends for the Customer (invites, reminders, receipts), with their address, content, and delivery status.
- Data of the Customer's members: name, email address, profile photo, role, and teams.
- Technical data: one-way hashes of IP addresses for rate limits. AllBack does not store IP addresses in clear text.

AllBack refuses forms that ask for passwords, one-time codes, bank login details, or payment card numbers. The Customer decides whether its forms collect special categories of personal data within the meaning of Art. 9 GDPR, and is responsible for a legal basis for it.

Categories of data subjects.

- People the Customer asks to fill in a form with a personal link.
- People who answer a form with an open link.
- Members of the Customer's organization on the Platform.

Duration. The term of the Main Agreement, and the periods for deletion in Section 8.

Annex 2: Technical and organisational measures

Access to the Platform.

- Sign-in with a 6-digit code by email, with no passwords. AllBack stores only a hash of the code. A code expires in minutes, and stops working after 5 wrong tries.
- Sign-in cookies that scripts cannot read, sent only over HTTPS. A session ends after 30 days, or when the person signs out.
- AI apps sign in with OAuth, and get a token for the account of the person who connects them, with no more rights than that person.
- Roles in each organization (owner, admin, and member) and teams. A member sees only their own requests and the requests of their teams.
- An audit log of the actions in each organization, for example invites, role changes, plan changes, and sending.

Access to Customer Data by the people who answer.

- Each personal link has 144 random bits, and shows only the prefilled data and the answers of that one person.
- On request of the Customer, a form opens only after a code sent to the person's own email address.
- Uploaded files are never public. Each download link is signed, and the links in exports expire after 7 days.

Separation.

- Forms run on their own domain (allback.app, with one subdomain for each organization), apart from the website and the accounts.
- The data of each organization is separated by the access rules of the Platform.
- Fully custom forms run in a sandbox with no network access and no access to cookies. AllBack checks every answer on its server.

Transmission and storage.

- HTTPS (TLS) for every request.
- The database and the uploaded files are stored in the European Union, in the EU jurisdiction of Cloudflare, and are encrypted at rest by Cloudflare.
- Strict content security rules: form pages run only AllBack's own scripts, send data only to AllBack, and cannot be embedded by other websites.

Availability and resilience.

- The Platform runs on the infrastructure of Cloudflare, with point-in-time recovery of the database.
- Limits on new forms, sign-in codes, and open-link answers stop automated abuse.

Data minimisation and deletion.

- No analytics and no advertising pixels on the Platform and the forms.
- AllBack does not sell Customer Data, and does not use it to train AI models.
- Unclaimed guest forms are deleted after 30 days. Demo answers are deleted after 30 minutes. An account is deleted when its owner asks.

Protection against abuse.

- AllBack refuses forms that ask for passwords, one-time codes, card numbers, or bank details.
- Automatic checks, including an AI review, look at new forms. People can report any form, and three reports close it at once.
- Every email has a link to stop the reminders and a link to report the form.

Organisation.

- Persons with access to Customer Data are bound to confidentiality.
- AllBack reviews these measures regularly, and adapts them to technical progress.

Annex 3: Sub-processors

- **Cloudflare, Inc.**, 101 Townsend St., San Francisco, CA 94107, USA. Hosting of the Platform and the forms, the database (D1) and the file storage (R2) in the EU jurisdiction, the store of the sign-ins of AI apps, and Workers AI and AI Gateway for the review of new forms. The database and the files stay in the EU. Other processing can take place in Cloudflare's global network. Transfer mechanism: EU–US Data Privacy Framework, and the EU Standard Contractual Clauses.

- **Plus Five Five, Inc.** (Resend), USA. Sending of the emails: invites, reminders, sign-in codes, and receipts. Data: the email address, the name, and the content of each email. Transfer mechanism: the EU Standard Contractual Clauses.
- **TypeSafe AI**, San Francisco, USA, through Cloudflare Workers AI and the AI Gateway. The AI review of new forms (the model Jev). Data: the text and the code of a new form, and the email address and the organization name of its sender. No answers of the people who fill in the form. Transfer mechanism: the EU Standard Contractual Clauses.
- **Google LLC**, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, through the Cloudflare AI Gateway. The AI review of new forms (Gemini). Data: the text and the code of a new form, and the email address and the organization name of its sender. No answers of the people who fill in the form. Transfer mechanism: EU–US Data Privacy Framework, and the EU Standard Contractual Clauses.