Data Processing Agreement

Version 1.1, 17 October 2026.

The short version

- You are the controller, we are the processor. We process personal data only to deliver what you bought, on your instructions, and for nothing else.
- Your data stays in the EU/EEA. Nothing trains on it. Every sub-processor is listed in Annex C and you can object to new ones.
- Read access by default, per named person, two-factor on, revoked when the work ends. A human approves every action our agents take in your systems.
- If something goes wrong we tell you without undue delay, with what, when and what we're doing.
- When we're done we delete or return everything, your choice, and confirm in writing.

The full text follows. It is the same for every client, accepted at checkout or on an order, with no signature needed. If your organisation has its own template, we usually accept yours instead.

1. Parties

Controller: the client named in the Agreement (the order, subscription or statement of work) that references this Data Processing Agreement, or that accepted it at checkout on minimumeffort.io.

Processor: Augmented Reality Studios AB, org.nr 559416-9426, C/O HVNT, Sturegatan 50, 114 36 Stockholm, Sweden, trading as Minimum Effort ("we", "us").

2. Definitions

Terms such as personal data, processing, controller, processor, sub-processor, data subject, personal data breach and supervisory authority have the meaning given in Regulation (EU) 2016/679 (the "GDPR"). "Agreement" means the order, subscription, statement of work or checkout under which we deliver services to you. "Services" means the services described in the Agreement. "Instructions" means your documented instructions, including this DPA, the Agreement, and written instructions given during the Services.

3. Scope and precedence

This DPA applies to all processing of personal data we carry out on your behalf in delivering the Services. It forms part of the Agreement. If this DPA and the Agreement conflict on the processing of personal data, this DPA prevails. If this DPA and the GDPR conflict, the GDPR prevails.

4. Subject matter, duration, nature and purpose

Set out in Annex A for each type of Service. In summary: we access and process personal data in your systems (such as mailboxes, calendars, CRM records, documents and operational data) to analyse how work is done, to build and run automations and tools, and to report on them. Processing lasts for the term of the Agreement plus the deletion period in section 12.

5. Our obligations as processor

We will:

1. process personal data only on your Instructions, unless required to by Union or Member State law, in which case we inform you before processing unless the law forbids it;
2. tell you without delay if we believe an Instruction infringes the GDPR or other data protection law;
3. ensure that every person authorised to process personal data has committed to confidentiality (section 7);
4. implement the technical and organisational measures in Annex B and maintain them for the term;
5. engage sub-processors only as set out in section 9;
6. assist you, taking into account the nature of the processing, in responding to requests from data subjects (section 10);
7. assist you with your obligations under GDPR Articles 32 to 36 (security, breach notification, impact assessments and prior consultation), taking into account the nature of the processing and the information available to us;
8. delete or return all personal data at the end of the Services as set out in section 12;
9. make available all information necessary to demonstrate compliance with GDPR Article 28 and allow for and contribute to audits (section 13).

6. Your obligations as controller

You confirm that you have a lawful basis for the processing you instruct us to carry out, that you have given the information required by GDPR Articles 13 and 14 to the data subjects concerned, and that your Instructions comply with data protection law. You are responsible for the accuracy and lawfulness of the personal data you give us access to. Where the Services include interviews with your employees (Annex A), you inform them in advance that the interviews are conducted with the help of an AI assistant and summarised for the purpose of the Services.

7. Confidentiality

Everyone who processes personal data under this DPA, employees and contractors alike, is bound by a written confidentiality obligation that survives the end of their engagement. Access is limited to the people who need it to deliver the Services.

8. Security

We implement the measures in Annex B, appropriate to the risk, including pseudonymisation and encryption where appropriate, confidentiality, integrity, availability and resilience of our systems, the ability to restore availability after an incident, and a process for regularly testing the measures. We may update Annex B as long as the overall level of protection does not decrease.

Two specific commitments:

- **No training.** Personal data we process for you is never used to train or improve machine learning models, ours or anyone else's. Our AI providers are contractually bound to the same rule.
- **Human approval.** Our automated agents may read, analyse and draft. Any action that sends a communication, changes data in your systems beyond the agreed automations, or affects a payment is executed only after approval by a named human, and the approval is logged.

9. Sub-processors

9.1 You give general authorisation for the sub-processors listed in Annex C, which we keep current at minimumeffort.io/dpa/agreement.

9.2 We notify you in writing (email to your contact in the Agreement) at least 14 days before adding or replacing a sub-processor. You may object on reasonable data protection grounds within that period. If we cannot address the objection, either party may terminate the affected Service without penalty for the remaining term, and section 12 applies.

9.3 We impose on every sub-processor, by written contract, data protection obligations equivalent to those in this DPA, and we remain fully liable to you for their performance.

10. Data subject rights

If we receive a request from a data subject concerning personal data processed for you, we forward it to you within 3 working days and do not respond ourselves unless you instruct us to. We assist you with identifying, correcting, exporting, restricting or deleting the data subject's personal data in the systems we have access to, within 10 working days of your request, at no extra cost where the effort is reasonable.

11. Personal data breach

We notify you without undue delay, and in any case within 36 hours of becoming aware of a personal data breach affecting personal data processed for you, so that you can meet your own 72-hour obligation under GDPR Article 33. The notification describes the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. We give further information as it becomes available, and we cooperate with you on any notification to the supervisory authority or data subjects. We do not notify a supervisory authority or data subjects on your behalf unless you instruct us to.

12. Deletion and return

Within 30 days after the end of the Services, or earlier on your request, we delete all personal data processed for you from our systems and those of our sub-processors, or return it to you in a commonly used format and then delete it, at your choice. Access credentials to your systems are revoked at the end of the Services. We confirm deletion in writing. We may retain personal data only where Union or Member State law requires it, for example invoicing records under the Swedish Bookkeeping Act, and only for as long as that law requires, under the same protections.

13. Audits

Once per 12 months, or after a personal data breach, you may audit our compliance with this DPA. You may do so by reviewing the documentation we provide (our security measures, sub-processor list, logs of access and approvals relating to your data), or, on 30 days' written notice, by an on-site or remote inspection by you or an independent auditor bound by confidentiality, during business hours, without unreasonable disruption. Each party bears its own costs. We answer written security questionnaires within 10 working days.

14. International transfers

Personal data is processed in the EU/EEA. Where a sub-processor in Annex C processes personal data outside the EU/EEA, the transfer rests on an adequacy decision (including the EU-US Data Privacy Framework for certified US providers) or on the European Commission's Standard Contractual Clauses with

supplementary measures, as noted in Annex C. We do not transfer personal data outside the EU/EEA on any other basis without your prior written consent.

15. Liability

Each party is liable to the other for damage caused by its breach of this DPA or the GDPR, within the limitations of liability in the Agreement, except that those limitations do not apply to fines or claims from data subjects to the extent caused by that party's breach of the GDPR, nor to damage caused by intent or gross negligence. Where both parties are liable to a data subject under GDPR Article 82, each party is liable towards the other for its share of the responsibility.

16. Term and termination

This DPA applies for as long as we process personal data for you, including the deletion period in section 12. Either party may terminate the Agreement for material breach of this DPA that is not cured within 14 days of written notice.

17. Changes

We may update this DPA to reflect changes in law or in our sub-processors, with 30 days' written notice. Changes that reduce your protection require your written agreement.

18. Governing law and disputes

Swedish law applies. Disputes are settled by the Stockholm District Court (Stockholms tingsrätt) as the court of first instance, after the parties have tried to resolve the matter between themselves.

19. Signatures

This DPA is accepted either by the Controller's acceptance at checkout on minimumeffort.io, by signature of the Agreement that references it, or by signature below.

Controller	**Processor**
Company:	Augmented Reality Studios AB
Org.nr:	559416-9426
Name:	Name:
Title:	Title:
Date:	Date:
Signature:	Signature:

Annex A: Details of processing

	Day One	The Audit (incl. month one of a subscription)	Build once, the 10-Day MVP, Subscriptions (Build and Run)
Subject matter	A prototype built from the Controller's brief	Analysis of how work is done in the Controller's organisation	Building and operating automations and tools in the Controller's systems
Nature	Receiving and storing a brief, brand material and references	Interviews with employees (recorded as summaries), read access to mailboxes, calendars, CRM, documents and operational systems in scope; analysis; building one automation	Read and, where agreed, write access to the systems in scope; building, running, monitoring and reporting on automations and tools
Purpose	Delivering the prototype	Producing the map, the ranked list and the quick win; the readout	Delivering and operating the agreed automations and tools; the monthly receipt
Duration	Until delivery plus 30 days	14 days plus 30 days	The term of the Agreement plus 30 days
Data subjects	The Controller's contact persons	Employees, customers, suppliers and other contacts of the Controller whose data appears in the systems in scope	Same as the Audit, for the systems in scope
Categories of data	Contact details; any personal data the Controller includes in the brief	Names, roles, contact details, communications (email, calendar), CRM records, documents, operational data; the content of employee interviews	Same as the Audit; data flowing through the automations (for example invoices, support requests, bookings)
Special categories	None intended. If the Controller's systems contain special categories of data, the Controller informs us in writing and we agree additional measures before access	Same	Same
Access	None to the Controller's systems	Read access to the systems listed in the kickoff; per named person; revoked at the readout	Read access by default; write access only to the systems and functions named in the Agreement; per named person; revoked at the end

Annex B: Technical and organisational measures

1. **Access control.** Access to the Controller's systems is granted per named person on our side, with two-factor authentication, never through shared accounts. Access is the minimum required and is revoked when the Services end or the person's involvement ends, whichever is first.
2. **Human approval of actions.** Our agents may read, analyse and draft. Actions that send communications, change data beyond the agreed automations, or affect payments require approval by a named human and are logged with who, what and when.
3. **Encryption.** Data in transit is encrypted (TLS 1.2 or higher). Data at rest in our systems is encrypted. Credentials and tokens are stored in a secrets vault, never in application tables or logs.
4. **Logging.** An append-only audit log records every access and every action by our agents and staff relating to the Controller's data. Logs are available to the Controller on request.
5. **Data minimisation.** We store the minimum needed to deliver the Services. Where we can work with references (such as a message id) instead of content, we do. Interview content is stored as summaries, not recordings, unless the Controller instructs otherwise.
6. **Segregation.** Each client's data is logically segregated with tenant-level access control in our systems.
7. **AI providers.** Prompts and outputs sent to AI providers are limited to what the task requires, are covered by data processing terms that exclude training, and are not retained by the provider beyond the

processing of the request except as the provider's terms state in Annex C.

8. **Staff and contractors.** Everyone with access is bound by confidentiality, trained on this DPA, and uses managed devices with disk encryption and screen lock.
9. **Backups and resilience.** Our systems are backed up with point-in-time recovery. Backups are encrypted and deleted on the same schedule as live data under section 12.
10. **Incident response.** We keep a written incident procedure covering detection, containment, notification under section 11, and review.
11. **Testing.** Measures are reviewed at least annually and after any incident.

Annex C: Sub-processors

Sub-processor	Service	Location	Transfer basis
Supabase, Inc.	Database, authentication, storage for HQ	EU (project region Frankfurt)	EU processing; SCCs for support access from outside the EU
Netlify, Inc.	Hosting and serverless functions	EU (functions region Dublin); CDN worldwide	EU-US Data Privacy Framework / SCCs
Google Ireland Limited (Google Workspace)	Email, calendar, documents	EU, with Google's global infrastructure	EU-US Data Privacy Framework / SCCs
Anthropic, PBC	AI processing of text for analysis and drafting; no training on inputs or outputs	US	EU-US Data Privacy Framework / SCCs
Stripe Payments Europe, Ltd.	Payments and invoicing (Controller's billing contact data only)	EU	EU processing
Fireflies.ai Corp. (only if the Controller agrees to call recording)	Meeting transcription	US	SCCs
Our accounting provider (named on request)	Bookkeeping (invoice data only)	Sweden	EU processing

This Annex is the current list, always at minimumeffort.io/dpa/agreement. Changes are notified under section 9.2.