Data Processing Agreement

under Art. 28 GDPR · Appendix to «Main Contract» no. «Contract number»

If the parties also sign the German version, the German version prevails in case of doubt.

CONTROLLER	PROCESSOR
«Company» **«Street»** **«Postcode City, Country»** **«Register court, register number»** represented by **«Name, function»** (“Controller”)	**Outcomet UG (haftungsbeschränkt)** Amalie-Baader-Straße 1 76137 Karlsruhe, Germany Amtsgericht Mannheim, HRB 758563 represented by its managing director Andy Görnt (“Processor”)

1 Subject matter and duration

The Processor operates the Outcomet software for the Controller as Software as a Service under **«Main Contract»** no. **«Contract number»** (the "Main Contract"). In doing so, it processes personal data on behalf of the Controller.

This agreement applies for as long as the Main Contract runs, and beyond that until all data has been deleted or returned under Section 10.

2 Nature, purpose and scope of processing

Purpose: providing Outcomet to collect, structure and analyse customer feedback, product content and decisions, including AI-assisted analysis.

Nature of processing: collecting, storing, organising, structuring, analysing, retrieving, transferring to the sub-processors in Annex B, deleting.

Types of personal data

- User account data: name, e-mail address, role, login data
- Content the Controller brings in: feedback, interview notes and transcripts, comments, product and strategy content, insofar as it relates to persons
- Contact data of the Controller's interviewees and customers: name, e-mail address, role, company, and the classifications the Controller or Outcomet stores about them in the workspace
- Data from integrations the Controller connects: issues, comments, commits and pull requests with author details
- E-mails that Outcomet sends on behalf of the Controller
- Usage and log data: IP address, browser data, error logs, session recordings with masked inputs

Categories of data subjects

- Employees and agents of the Controller whom it invites as users
- Customers, users and interviewees of the Controller whose data it brings in
- Persons who appear as authors or editors in systems the Controller connects

Outcomet does not process special categories of data under Art. 9 GDPR as intended use. The Controller does not bring in such data.

3 Instructions

The Processor processes the data only on documented instructions from the Controller. This agreement, the Main Contract and the Controller's use of Outcomet's features are such instructions. The Controller gives further instructions in text form.

If the Processor considers an instruction unlawful, it informs the Controller without undue delay.

There is no processing for the Processor's own purposes. In particular, the Controller's data is not used to train AI models, neither by the Processor nor by its sub-processors. The only exception to processing for own

purposes concerns TypeSafe: aggregated statistics and insights from the requests, no model training (Annex B). The Controller consents to it with this agreement.

4 Confidentiality

All persons at the Processor who have access to the data are bound to confidentiality. At present, only the managing director has access to the data in the Solution. Anyone reading along in a channel shared with the Controller is bound to confidentiality in writing. Further persons receive access only after a written confidentiality commitment.

5 Security of processing

The Processor takes the technical and organisational measures under Art. 32 GDPR described in Annex A. It may develop them further as long as the level of protection does not decrease.

6 Sub-processors

The Controller approves the sub-processors in Annex B.

The Processor informs the Controller in text form at least 30 days in advance of new or replaced sub-processors. Within this period, the Controller may object for an important data protection reason. If the parties do not agree, the Controller may terminate the Main Contract as of the date of the change.

The Processor contractually binds every sub-processor to an equivalent level of data protection. The sub-processors' own service providers follow their published lists, which Annex B names.

7 Transfers to third countries

The database with all of the Controller's content is located in the EU. Some sub-processors process data in the USA or the United Kingdom (Annex B). The basis in each case is an adequacy decision of the EU Commission, including the EU-US Data Privacy Framework, or the EU Standard Contractual Clauses.

8 Assistance to the Controller

The Processor assists the Controller with requests from data subjects (Art. 12 to 23 GDPR) and with its obligations under Art. 32 to 36 GDPR. It forwards requests received directly by the Processor without undue delay.

9 Personal data breaches

The Processor notifies the Controller of a breach without undue delay, at the latest 48 hours after becoming aware of it. The notification contains, as far as known, the information under Art. 33(3) GDPR.

10 Deletion and return

After the end of the Main Contract, the Controller can export its data for 30 days. The Processor then deletes it, including in the development environment, unless a statutory retention obligation applies. Copies in backups are overwritten in the regular backup cycle. For sub-processors, deletion follows Annex B. The Processor deletes messages in a shared channel on request.

11 Evidence and audits

The Processor provides the Controller with the information needed to demonstrate compliance with this agreement. It allows audits by the Controller or an auditor appointed by it and bound to confidentiality, with at least 14 days' notice, during normal business hours and at most once a year, unless there is a specific reason.

12 Relationship to other agreements and final provisions

Liability is governed by Art. 82 GDPR. Otherwise, the liability provisions of the Main Contract apply.

In case of conflict, this agreement prevails over the Main Contract and over any non-disclosure agreement (NDA) between the parties, insofar as the processing of personal data is concerned. Using the sub-processors named in Annex B does not breach such an NDA.

Changes require text form. German law applies, the place of jurisdiction is Karlsruhe.

CONTROLLER **«Company»**	PROCESSOR **Outcomet UG (haftungsbeschränkt)**
PLACE	PLACE Karlsruhe
DATE	DATE
NAME, FUNCTION **«Name, function»**	NAME, FUNCTION Andy Görnt, Geschäftsführer (Managing Director)
SIGNATURE	SIGNATURE

A Annex A · Technical and organisational measures under Art. 32 GDPR · as of 31 October 2026

The Processor is a micro-enterprise. The measures are designed for that: few people with access, security through the sub-processors' platforms, everything traceable.

1 Confidentiality

Physical access: Outcomet does not operate its own servers. The data centres belong to the providers in Annex B, which demonstrate their physical security under SOC 2 Type II or ISO 27001.

Access to systems

- Only the managing director has administrative access to the database, hosting and provider accounts.
- Credentials for programming interfaces are stored as environment variables at the respective provider, not in the source code.
- Users log in with e-mail and password or through an identity provider. Login is managed by Supabase Auth.

Access to data

- Customer data is separated at workspace level. Row-level security is active on all tables in the production database. A user only sees data of the workspaces they are invited to.
- New users are invited by an administrator of the Controller. Users with an e-mail address under the Controller's domain are assigned to its workspace automatically.
- The Controller connects integrations (GitHub, Jira, HubSpot, Granola, LinkedIn, Discord) itself via OAuth and can disconnect each of them individually. AI clients it connects through the Outcomet MCP server are set up by the Controller itself, which can revoke their access at any time.

Separation

- Production and development environments are separate database projects, both in the EU.
- The development environment is filled with a full copy of the production data to reproduce errors under real conditions. The same access rules apply to it. Only the managing director has access.

Pseudonymisation: inputs in form fields are masked in session recordings. Content is currently not pseudonymised before AI processing. Data that the Controller brings in already pseudonymised stays pseudonymised.

2 Integrity

Transfer

- All connections are encrypted with TLS: browser, interfaces and connections to sub-processors.
- Supabase encrypts stored data with AES-256.
- Content only goes to the sub-processors in Annex B, and only through business API access, never through consumer products.

Input control

- Content created by users carries its creator and the time of the last change. Data from integrations carries its origin. There is no complete per-field change log.
- AI calls are logged with function, model, workspace and time.
- Logins and server access are logged by the hosting providers.

3 Availability and resilience

- Daily backups by Supabase, kept for seven days.
- The Controller can export its data at any time.
- Error monitoring (Sentry, EU) reports errors and outages immediately.
- Schema changes run through versioned migrations in the source code repository.

4 Review and evaluation

- Changes to the source code go through pull requests with automated checks and code review before merging.
- The database provider's security advisories (Supabase Advisor) are reviewed regularly.
- This annex and Annex B are updated with every change to providers or data flows, at least once a year.

5 Control of processors

- An agreement under Art. 28 GDPR is in place with every sub-processor; for transfers to third countries with Standard Contractual Clauses or on the basis of an adequacy decision.
- The Controller's data is not transferred to private accounts or to tools without a data processing agreement.
- No sub-processor may use the data to train AI models.

6 Personal data breaches

- The managing director examines a suspected breach immediately.
- Notification to the Controller without undue delay, at the latest 48 hours after becoming aware, under Section 9 of the agreement.
- Contact: andy@crew.outcomet.app

B Annex B · Sub-processors · as of 31 October 2026

The database with all of the Controller's content is located in the EU.

Core operations

PROVIDER	PURPOSE	DATA	PLACE OF PROCESSING	BASIS FOR THIRD COUNTRY
Supabase Inc., USA	Database, login, file storage, server functions	all account and content data	EU (Paris); development environment EU (Frankfurt)	not required for storage; Standard Contractual Clauses for support access from the USA
Netlify Inc., USA	Delivery of the application; forwarding of error reports to Sentry	IP address, technical request data, error reports	global network, delivery from the nearest location; company in the USA	Standard Contractual Clauses
API Hero Ltd (Trigger.dev), United Kingdom	Background processing, AI workflows	content during processing	execution EU (Frankfurt, AWS eu-central-1); run and log data on the provider's platform, location not guaranteed	Standard Contractual Clauses
Resend Inc., USA	Sending and receiving e-mails in Outcomet	e-mail address, message content	sending and receiving EU (Ireland, AWS eu-west-1); account and log data possibly with the provider in the USA	Standard Contractual Clauses, EU-US Data Privacy Framework
Functional Software Inc. (Sentry), USA	Error monitoring, session recording with masked inputs	technical data, user ID, screen recording of individual sessions	EU (Frankfurt)	Standard Contractual Clauses, EU-US Data Privacy Framework
Slack Technologies Ltd., Ireland (Salesforce group)	Communication with the Controller where a shared channel is agreed	name, e-mail address and profile of participants; messages and files the Controller shares in the channel	USA (provider's data storage)	Standard Contractual Clauses
Google Cloud EMEA Ltd., Ireland (Google Workspace)	E-mail, calendar and video meetings with the Controller	name and e-mail address of participants; content of e-mails and meetings	EU and USA (provider's data centres)	Standard Contractual Clauses
Granola Inc., USA	Notes and transcripts of meetings with the Controller	meeting content; names and e-mail addresses of participants	USA	Standard Contractual Clauses

AI processing

Content goes exclusively through business API access. None of these providers trains models with the Controller's data.

PROVIDER	PURPOSE	DATA	LOCATION	STORAGE AT THE PROVIDER	BASIS
Anthropic PBC, USA	Analysis, summaries, assistant (Claude)	feedback, interview content, product content, chat histories	USA	up to 30 days for abuse detection	Standard Contractual Clauses
OpenAI Ireland Ltd., Ireland, with OpenAI OpCo, LLC, USA	Classification, metadata, embeddings for search	text content	USA	up to 30 days for abuse detection	Standard Contractual Clauses
TypeSafe AI, Inc., USA	Classification of feedback, content sources and changes (model "Jev")	feedback text, name of the reporting person, transcript sections; name, e-mail address, role and company of interview participants with their classifications and up to five earlier signals; title, description and file names of changes; source content	USA (AWS; compute nodes at Modal, Nebius, CoreWeave)	no storage on the compute nodes; no contractual commitment on duration for the database	Standard Contractual Clauses, Modules 2 and 3

Exception under Section 3 · TypeSafe

TypeSafe may use aggregated statistics, classifications, metrics and insights derived from the requests for its own service and products (TypeSafe Master Customer Agreement § 4.3). Model training with the content is excluded without consent (§ 4.1). The classification results belong to the Processor (§ 11) and are stored only in the Controller's workspace.

TypeSafe is an integral part of classification in Outcomet. By signing this agreement, the Controller consents to this exception.

Services for reading public websites

These services only receive addresses of public websites, no content and no personal data of the Controller. They are therefore not sub-processors. They are listed for completeness.

PROVIDER	FUNCTION	SEAT
SideGuide Technologies, Inc. (Firecrawl)	Product Context and Competitor Context: reading the website the Controller enters	USA
Jina AI GmbH (Elastic)	as Firecrawl, as fallback	Berlin
Microlink	Link preview for content sources	Spain

Not sub-processors

The Controller connects GitHub, Atlassian (Jira), HubSpot, Granola (as the Controller's own integration), LinkedIn and Discord itself via OAuth. They act towards the Controller as providers in their own right. Each connection can be disconnected individually at any time. The same applies to AI clients the Controller connects through the Outcomet MCP server: they receive only the data the Controller requests through them.

Service providers of the sub-processors

Each provider above uses its own service providers and publishes them. Their lists are authoritative, among others:

- Supabase: https://supabase.com/legal/customer-resources/subprocessor-list
- Sentry: https://sentry.io/legal/subprocessors/
- Resend: https://resend.com/legal/subprocessors
- OpenAI: https://openai.com/policies/sub-processor-list/
- TypeSafe: https://trust.typesafe.ai/subprocessors
- Anthropic, Netlify, Trigger.dev: via the provider's privacy or DPA page