CAARD Data Processing Agreement

Agreement on the processing of personal data on behalf of a controller under Art. 28 GDPR (Auftragsverarbeitungsvertrag). Version 1.0, effective 16 November 2026. The current version is published at https://www.caard.net/dpa.

1. Parties

Controller: _____ (company name), _____ (address), _____ (register court and number) (the "Customer").

Processor: CAARD UG (haftungsbeschränkt), Bauerngasse 103, 97421 Schweinfurt, Germany, registered at Amtsgericht Schweinfurt under HRB 9727, represented by its managing director Dhairya Kamal Shah ("CAARD").

This agreement forms part of the agreement under which the Customer subscribes to CAARD, such as CAARD's Terms of Service (caard.net/terms), an offer, an order form or a subscription (the "Main Agreement"). If the two conflict on data protection, this agreement prevails.

2. Subject matter and duration

CAARD provides a lead capture and follow-up service for sales and event teams: mobile apps for iPhone and Android, a mobile web app (app.caard.net) and a web dashboard (dash.caard.net). CAARD processes personal data only to provide this service to the Customer.

This agreement runs for as long as CAARD processes personal data for the Customer. It ends once that processing has ended and the data has been deleted or returned under clause 11.

3. Nature, purpose and scope of processing

Nature of processing: collection, recording, storage, structuring, retrieval, transcription, enrichment, scoring, transmission to systems the Customer connects, and deletion.

Purposes:

1. Capturing contacts from business cards, event badges, LinkedIn QR codes, manual entry and CSV import.
2. Reading contact details from photos and transcribing voice notes and meeting recordings with AI.
3. Enriching contacts and companies with professional information from public web sources. Leads added from a LinkedIn QR code are enriched automatically unless the user turns this off; other enrichment runs when a user starts it or an admin schedules it.
4. Scoring leads against an ideal customer profile the Customer defines.
5. Drafting follow-up emails, sending them through the Customer's connected mailbox, and syncing leads to the Customer's CRM, calendar and Slack, if connected.
6. Finding companies and contacts that match criteria the Customer sets (Lead Finder and event research).
7. Running the Customer's workspace: user accounts, roles, billing seats and support.

Categories of data subjects:

- The Customer's users: employees and contractors who sign in to CAARD.
- Contacts captured by those users: prospects, customers, partners and other people met at events or in meetings.
- Other participants in meetings the Customer records.

Categories of personal data:

- Users: name, email address, username, profile photo, role and team membership, settings, sign-in and device data, usage events and error reports.
- Contacts: name, job title, company, email addresses, phone numbers, postal address, website, LinkedIn and other public profiles, profile photo, card and badge photos, notes, tags, custom fields, follow-up tasks, emails sent from CAARD, voice notes and their transcripts, the place and time a lead was saved (if location capture is on), enrichment results and lead scores.
- Meetings: transcripts and summaries of meetings the Customer records. The audio is deleted once transcribed.

No special categories of personal data under Art. 9 GDPR are intended to be processed. The Customer instructs its users not to record such data in notes or meetings.

Place of processing: CAARD is based in Germany. Several subprocessors, including the database and the AI providers, process data in the USA. Annex 2 lists each subprocessor, its location and the transfer mechanism.

4. Customer instructions

CAARD processes personal data only on the Customer's documented instructions. The Main Agreement, this agreement and the settings the Customer chooses in CAARD are the Customer's instructions; examples are turning enrichment on, connecting a CRM and deleting a lead. Further instructions must be given in text form.

CAARD informs the Customer without delay if it believes an instruction infringes data protection law. CAARD may suspend that instruction until the Customer confirms or changes it.

If EU or member-state law requires CAARD to process data in another way, CAARD informs the Customer before processing, unless that law prohibits it.

5. Confidentiality

CAARD ensures that everyone authorised to process the personal data is committed to confidentiality or is under a statutory duty of confidentiality. This duty continues after their work for CAARD ends.

6. Security of processing

CAARD implements the technical and organisational measures in Annex 1 to ensure a level of security appropriate to the risk (Art. 32 GDPR). CAARD may update these measures as technology develops, provided the level of protection does not fall. CAARD documents material changes and makes them available to the Customer on request.

7. Subprocessors

The Customer gives general written authorisation for CAARD to engage subprocessors. The subprocessors in Annex 2 are approved on conclusion of this agreement.

CAARD publishes its current list of subprocessors at https://dash.caard.net/en/legal/subprocessors.

CAARD informs the Customer of any intended addition or replacement of a subprocessor at least 30 days in advance, by email to the Customer's workspace admins. The Customer may object in text form within those 30 days on reasonable data protection grounds. If the parties can't resolve the objection, the Customer may terminate the affected part of the service without penalty.

CAARD binds each subprocessor to data protection obligations at least as protective as this agreement, except where Annex 2 states otherwise. CAARD remains liable to the Customer for its subprocessors' performance of those obligations.

Services the Customer connects itself are not CAARD's subprocessors: for example its CRM, mailbox, calendar, Slack, or its own Apollo or RocketReach account. CAARD sends them data on the Customer's

instruction, and they process it under the Customer's own agreement with them.

8. Transfers outside the EU/EEA

CAARD transfers personal data to countries outside the EU/EEA under Chapter V GDPR. Each recipient is certified under the EU–US Data Privacy Framework, covered by another adequacy decision, or bound by the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), with supplementary measures where needed. The exception is Exa, for which no transfer mechanism is in place yet. Annex 2 names the mechanism for each subprocessor and says what Exa receives.

9. Assistance to the Customer

CAARD assists the Customer, through the product and on request, in responding to data subjects exercising their rights under Art. 12–23 GDPR. In the product, workspace admins can view, correct, export (CSV) and delete leads. If a data subject contacts CAARD directly about data CAARD processes for the Customer, CAARD forwards the request to the Customer without delay and does not answer it on its own.

CAARD also assists the Customer in meeting its obligations under Art. 32–36 GDPR: security, breach notification, data protection impact assessments and prior consultation. This assistance takes into account the nature of the processing and the information available to CAARD.

10. Personal data breaches

CAARD notifies the Customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting the Customer's data. The notice contains what CAARD knows at the time:

- the nature of the breach;
- the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures taken or proposed to address the breach and limit its effects.

CAARD provides further information as it becomes available.

11. Deletion and return of data

When the Main Agreement ends, the Customer may export its leads as CSV for 30 days. CAARD then deletes the Customer's personal data, unless EU or member-state law requires CAARD to keep it. Copies in backups are deleted when those backups expire in the normal backup cycle.

During the term, deletion works as follows:

- Deleted leads go to the workspace's trash and are permanently deleted after 90 days, or sooner when the trash is emptied, including card photos and voice recordings.
- Lead activity history is kept for 60 days.
- Voice notes recorded online are not stored after transcription.
- Meeting recordings are deleted as soon as they are transcribed. Transcripts and summaries are kept until the Customer deletes them.

12. Audits and information

CAARD makes available to the Customer the information needed to demonstrate compliance with Art. 28 GDPR. CAARD allows for and contributes to audits, including inspections, by the Customer or an auditor the Customer mandates.

Audits take place at most once a year, unless a personal data breach or a supervisory authority requires otherwise. The Customer gives at least 30 days' notice, and audits take place during business hours without disrupting CAARD's operations. The auditor must be bound to confidentiality. Each party bears its own costs.

CAARD may first answer an audit request with written information, current documentation, or the certifications and audit reports of its subprocessors.

13. Liability

The parties are liable to data subjects as set out in Art. 82 GDPR. Between the parties, CAARD's total liability under this agreement is limited to the fees the Customer paid to CAARD in the 12 months before the event giving rise to the claim.

This limit does not apply to liability for intent or gross negligence, for injury to life, body or health, or where liability cannot be limited by law.

14. Final provisions

Changes and additions to this agreement must be made in text form. If a provision is or becomes invalid, the rest of this agreement remains valid, and the statutory provisions apply in place of the invalid one.

This agreement is governed by the laws of the Federal Republic of Germany. The place of jurisdiction is Schweinfurt, Germany, to the extent permitted by law.

Annex 1: Technical and organisational measures

CAARD runs entirely on managed cloud infrastructure and operates no servers or data centres of its own. Physical security therefore rests with the hosting subprocessors in Annex 2. The measures below are the ones CAARD controls.

1. Confidentiality

Physical access control

- Customer data is stored with Convex on Amazon Web Services and served through Vercel. Both run in data centres certified to ISO 27001 and audited under SOC 2.
- CAARD staff laptops use full-disk encryption and a screen lock.

System access control

- Sign-in runs through Clerk. Passwords are stored only as secure hashes by Clerk and never reach CAARD.
- Users can turn on two-factor authentication and passkeys on the web dashboard. Sign in with Apple is available on iPhone.
- Sign-ins from an unrecognised device require an email verification code.
- Sessions use short-lived signed tokens (JWT), which the backend verifies on every request.

Data access control

- Every Customer workspace is a separate tenant. Every backend function checks that the caller belongs to the workspace whose data it touches.
- Within a workspace there are two roles. Admins manage members, integrations and settings; members can only access the leads they are permitted to see.
- Uploaded files (card photos, voice recordings, profile photos) are bound to the workspace that uploaded them. The backend refuses access to them from any other workspace.
- Tenant isolation was last tested in an internal security review in October 2026, with live attempts to read and change another workspace's data. The issues found were fixed and re-tested before release.

- Access to production systems (database, sign-in, hosting and AI provider consoles) is limited to CAARD's founders. Every such account uses two-factor authentication.
- Administrative actions in CAARD's internal admin console are written to an audit log.

Separation control

- Production and development run on separate database deployments, separate sign-in instances and separate API keys.
- Demo and test data are kept in separate workspaces that contain only fictional records.

Encryption

- All connections use TLS: between the apps and CAARD, and between CAARD and its subprocessors.
- The database provider encrypts all data at rest (AES-256).
- Credentials for connected services (CRM and mailbox tokens, Apollo and RocketReach API keys) are additionally encrypted by CAARD with AES-256-GCM before storage. The keys are held only in the production environment configuration.

2. Integrity

Transfer control

- Personal data leaves CAARD only to the subprocessors in Annex 2, for the task at hand, and to services the Customer connects itself.
- Each AI request contains only the data its task needs, for example one card photo or one lead's details.
- Product analytics never receive contact data. Session replays in error monitoring mask all text and images.

Input control

- Each lead records who created it and when. Changes to a lead are written to its activity history, kept for 60 days.
- Administrative actions are written to an audit log.

3. Availability and resilience

- The backend, database and web apps run on managed platforms with redundancy across availability zones.
- The production database is backed up on a regular schedule.
- The iPhone and Android apps keep captured leads on the device until they sync, so a network or backend outage loses no captures.
- Error monitoring alerts the team to failures in the web dashboard.
- Rate limits on AI and enrichment functions protect against abuse.

4. Regular review and data protection by default

Testing. Changes pass automated tests before release. The web app and backend are reviewed for security periodically; the last review was in October 2026.

Data protection by default.

- Scheduled enrichment and the paid contact lookup are off until an admin turns them on. Location capture runs only after the user grants the device's location permission. Leads added from a LinkedIn QR code are enriched automatically; each user can turn this off.
- Voice notes recorded online are transcribed and not stored. Meeting recordings are deleted once transcribed.
- The iPhone and Android apps contain no analytics, advertising or tracking SDKs.
- Web analytics run in the EU with automatic click capture and session recording turned off.

Deletion.

- Deleted leads are permanently deleted from the trash after 90 days by a daily job, including card photos and voice recordings.
- Lead activity history older than 60 days is deleted by a daily job.
- Deleting a user account removes the sign-in account at once. The profile, personal workspace, connected mailboxes and assistant conversations are removed within minutes.
- Deleted data can remain in backups until those backups expire.

Incident response. Suspected incidents are reported to dhairya@caard.net and assessed by the managing director. Affected customers are notified under clause 10.

Subprocessor management. CAARD reviews a provider's security certifications and data protection terms before engaging it as a subprocessor.

Annex 2: Subprocessors

CAARD uses nine subprocessors for Customer data. Seven process data in the USA. Product analytics (PostHog) and error monitoring (Sentry) are hosted in the EU.

Subprocessor	Purpose	Personal data	Location	Transfer mechanism
Convex, Inc.	Database, file storage, backend functions	All Customer data described in clause 3	USA (AWS us-east-1)	SCCs, Module 2, in Convex's DPA, which is part of its Terms of Service
Clerk, Inc.	Sign-in and user accounts	Users' name, email address, password hash, sessions, device data	USA	Data Privacy Framework
Vercel Inc.	Hosting of the web dashboard and mobile web app	Data passing through the web apps; IP addresses	USA, with a global edge network	Data Privacy Framework
OpenAI Ireland Ltd, with processing by OpenAI, L.L.C.	Reading cards and badges, transcription, email drafts, enrichment, lead scoring, the in-app assistant, meeting summaries	Card photos, audio, lead details, meeting transcripts	USA	OpenAI's DPA, which applies to all API use, with OpenAI Ireland Ltd as the contracting party; onward transfer to the USA under SCCs. Not used to train models; kept for up to 30 days for abuse monitoring, then deleted
ElevenLabs, Inc.	Live dictation; transcription of voice notes and meetings	Audio and transcripts	USA	Data Privacy Framework and SCCs
Exa Labs, Inc.	Web search and reading public web pages for enrichment, Lead Finder, event research, LinkedIn QR codes and company briefs in the assistant; optional paid contact lookup (off by default)	Contact name, company, job title, LinkedIn URL; company websites	USA	None in place yet; see the note below the table

Subprocessor	Purpose	Personal data	Location	Transfer mechanism
Stripe Payments Europe, Ltd	Billing for paid workspaces	Billing contact's name and email address; card data goes directly to Stripe	Ireland, with processing in the USA	Data Privacy Framework
PostHog, Inc.	Product analytics on the web dashboard; never receives contact data	User ID, name, email address, workspace, usage events	EU (Frankfurt)	Hosted in the EU
Functional Software, Inc. (Sentry)	Error monitoring for the web dashboard	IP address, browser, page and error details; replays with all text and images masked	EU (Frankfurt)	Hosted in the EU

Exa. Exa does not offer data processing terms on CAARD's current plan, so no Article 28 agreement and no SCCs are in place with it yet. CAARD sends Exa business details only: a contact's name, company, job title and public LinkedIn URL, and public company websites. Exa's terms allow it to use search queries to improve its services. CAARD is seeking data processing terms from Exa and will update this annex when they are in place. If the Customer objects, CAARD will work with it to switch off the features that use Exa for its workspace, and clause 7's objection right applies.

Other services. The apps and backend call these services for single lookups:

Service	Data it receives	Purpose
unavatar.io	A contact's LinkedIn handle	Finds the contact's public profile photo
Google (favicon service, Public DNS)	Company domains	Shows company logos and checks that email domains exist
OpenStreetMap Nominatim, Photon (komoot), CARTO, OpenFreeMap	Coordinates where a lead was saved; place searches	Place names and maps
Apple (iPhone only)	Voice audio, processed on the device where possible	Fallback speech recognition when live transcription is unavailable

Services the Customer connects. These are not CAARD's subprocessors. They process data under the Customer's own agreement with them: Gmail, Microsoft Outlook, HubSpot, Salesforce, Zoho, Odoo, Attio, Pipedrive, Microsoft Dynamics 365, monday.com, Slack, Calendly, Cal.com, HubSpot Meetings, Chili Piper, and the Customer's own Apollo or RocketReach account. Follow-up emails are sent through the Customer's own connected mailbox.

Signatures

	Customer (Controller)	CAARD UG (haftungsbeschränkt) (Processor)
Name		Dhairya Kamal Shah
Title		Managing Director
Place, date		Schweinfurt,
Signature		