

Data Processing Agreement

DPA | GDPR Article 28 | October 13, 2026

1. Parties, Roles, and Purpose

This DPA is entered into between the Customer identified in the order, acting as controller or as a processor duly authorized by its controller, and GROUPE GARAN, a French SAS with share capital of EUR 100, Paris Trade and Companies Register No. 953 558 582, 200 rue de la Croix Nivert, 75015 Paris, France, which operates Beeving.

Beeving acts, respectively, as processor or subprocessor for the processing described in Appendix 1. The GDPR, Regulation (EU) 2016/679, and applicable data protection laws govern these operations. GDPR terms retain their statutory meanings.

Processing determined by GROUPE GARAN to administer its own customer relationship, bill customers, or manage its website is described in the Privacy Policy. That processing does not become processing on instructions solely because of this DPA.

2. Documented Instructions

Beeving processes data only on the Customer's documented instructions, including instructions concerning international transfers. They include the order, enabled features and settings, integration permissions, authorized campaigns, and lawful written instructions.

If Union or Member State law requires different processing, Beeving informs the Customer before the operation, unless prohibited by law on important public interest grounds. Beeving immediately informs the Customer if an instruction appears to conflict with data protection rules.

No instruction permits circumvention of individuals' rights, provider restrictions, or Google Limited Use rules. Beeving does not reuse Customer data for its own outreach, a shared commercial database, or training general-purpose models solely on the basis of this DPA.

3. Customer Obligations

The Customer determines an appropriate legal basis, informs individuals, holds the necessary rights over the data, and honors their requests. It documents instructions, manages users, and minimizes data imported, enriched, or sent to models.

The Customer does not import special categories of data or criminal-offense data without an appropriate framework and agreed safeguards. High-risk decisions and uses require the necessary assessments and controls. These obligations do not exclude any obligation belonging to Beeving.

4. Confidentiality and Security Measures

Beeving restricts access to authorized individuals subject to a statutory or contractual confidentiality obligation, during and after their roles. It limits access according to need and manages permissions and secrets.

Beeving implements technical and organizational measures appropriate to the state of the art, costs, nature of the data, and risks, in accordance with GDPR Article 32. Appendix 3 describes the framework for these measures. Beeving maintains their level of protection and does not substantially reduce it during processing.

5. Subprocessors

The Customer generally authorizes the subprocessors identified in Appendix 2, only for the necessary operations and data. Beeving enters into agreements with them imposing the same relevant data protection obligations and remains responsible to the Customer for their performance.

Beeving gives written notice to the account administrator of any addition or replacement at least thirty days before the new processing begins. The Customer may object before that date on reasonable data protection grounds. The parties seek an appropriate solution before the disputed processing starts.

If no solution is reached, the relevant processing or service may end without requiring acceptance of the new recipient. The prepaid, unused portion corresponding to that service is refunded. Mandatory obligations and data subjects' rights remain applicable.

A provider acting for its own purposes, including Apollo for its business database, is not covered for those purposes by a simple authorization to engage subprocessors. A separate disclosure requires an assessment of roles, a legal basis, information, and appropriate transfer safeguards. Beeving cannot impose it as a new implied instruction.

6. Individual Rights

Taking account of the nature of the processing, Beeving assists the Customer, through appropriate technical and organizational measures, in responding to requests for access, correction, erasure, restriction, portability, objection, and withdrawal of consent.

A request received directly concerning Customer data is forwarded without undue delay to the appropriate contact. Beeving does not independently respond to the substance of the request, except on documented instructions or where required by law. It retains the information needed for follow-up and complies with the Customer's lawful instructions.

7. Assistance with Security and Assessments

Beeving helps the Customer comply with GDPR Articles 32 through 36, taking account of the nature of the processing and the information available to it: security, breach notification, communication to individuals, impact assessments, and prior consultation.

Specific assistance arrangements are agreed in good faith. They cannot delay an urgent legal obligation or negate this DPA's assistance obligations. Any costs of an additional service are disclosed and accepted before it is performed.

8. Personal Data Breaches

Beeving notifies the Customer of any breach involving its data without undue delay after becoming aware of it, using the account's administrator or data protection contact. It takes appropriate steps to contain the incident, preserve relevant information, and limit its consequences.

As information becomes available, the notice states the nature and timing of the incident, categories of individuals and data, approximate volumes, likely consequences, measures taken or proposed, and the operational contact.

The immediate unavailability of complete information does not delay the initial notice. Additional details are communicated progressively. The Customer determines its own notifications to the authority and individuals with Beeving's assistance; this DPA does not transfer Beeving's own obligations to the Customer.

9. Return, Closure, and Deletion

At the end of the processing services, Beeving returns or deletes the data at the Customer's choice, then deletes copies, unless retention is required by applicable Union or Member State law. Return is secure and uses a commonly used, machine-readable format appropriate to the data.

After account deletion, production data is erased within thirty days at the latest; backups are erased within ninety days at the latest, measured from the same date. Any legally applicable retrieval period is taken into account before closure, unless lawful early deletion is instructed.

While awaiting purge, backups remain protected and are not used for routine operations, outreach, or further analysis. If a restore is necessary, deletion instructions are reapplied before the relevant data is returned to operational use.

Data whose retention is required is isolated and processed only for that obligation during the applicable period. Beeving confirms deletion on request and forwards relevant instructions to its subprocessors. Shorter mandatory deadlines prevail when applicable.

Data held in the Customer's email accounts, by recipients, or in a database controlled by a third party is not automatically erased by Beeving. The Customer continues to receive assistance in identifying necessary steps, without presenting these independent copies as Beeving backups.

10. International Transfers

Transfers outside the EEA and access from third countries take place only on documented instructions and after a valid mechanism under GDPR Chapter V has been implemented. European hosting does not remove the need to assess remote access and recipients.

Where appropriate, the European Commission's standard contractual clauses are entered into according to the actual roles, together with a transfer assessment and any necessary supplementary measures. An adequacy decision is relied on only if it actually covers the recipient and processing.

Beeving provides the Customer with information relevant to verifying transfers and safeguards. This DPA does not, by itself, constitute a standard contractual clause for transfers to a third country. An instruction or service authorization does not replace the required legal mechanism.

11. Information, Audits, and Inspections

Beeving makes available the information necessary to demonstrate compliance with Article 28 and allows and contributes to audits, including inspections, by the Customer or its appointed auditor.

Arrangements may include reasonable notice, appropriate confidentiality, and protection of other customers. They cannot prevent effective verification, an urgent audit justified by a breach, or an inspection required by a competent authority.

Available documentation may support preparation for the audit without categorically replacing a necessary inspection right. Any finding of noncompliance leads to a corrective action plan appropriate to the risk.

12. Term, Priority, and Acceptance

The DPA applies while processing is performed for the Customer and during operations necessary for closure, return, and deletion. Confidentiality and obligations concerning lawfully retained data continue for as long as necessary.

The DPA prevails over conflicting Terms concerning Customer data. Google data restrictions remain applicable. No contractual cap limits a mandatory data protection right or a data subject's remedy.

The DPA may be accepted electronically with the order or signed separately. The Customer and its contacts are identified through the account and order; a separate handwritten signature is not necessary when valid electronic acceptance is retained. Beeving contact: contact@beeving.com.

Appendix 1. Description of Processing

Item	Scope
Subject Matter and Purposes	Provide enabled campaign, newsletter, sequence, CRM, email, enrichment, and AI assistance features in accordance with the Customer's instructions.
Operations	Collection and import, recording, organization, storage, consultation, enrichment, generation, analysis, sending, receipt, synchronization, export, correction, and deletion.
Data Subjects	The Customer's users and staff; prospects and business contacts; the Customer's subscribers and customers; other individuals included in authorized communications.
Data Categories	Identity and contact details, company and job title, CRM fields, tags and notes, lists and objections, message content and metadata, relevant attachments, events, statistics, AI instructions, and necessary technical identifiers.
Special Data	No intentional processing of sensitive data or criminal-offense data without documented agreement and specific safeguards. Text and attachments must be minimized.
Duration	Period of the enabled Service, closure, and return; after account deletion, a maximum of 30 days in production and 90 days in backups, except for a limited statutory exception.
Instructions and Frequency	Operations requested by the Customer through the interface, APIs, integrations, and written instructions; according to feature scheduling and use.

Appendix 2. Authorized Providers and Separate Services

Provider	Function, Role, and Location
Amazon Web Services	Infrastructure and hosting processing. Platform hosted in the EU; EMEA entity in Luxembourg and any international access subject to appropriate safeguards.
Cloudflare, Inc.	Protection and distribution processing for relevant traffic or content; entity in the United States and global network. Scope limited to the operations actually provided.
OpenRouter	Processing to route AI requests to the providers used; access or transfers outside the EEA may occur.
Anthropic, OpenAI, Google, and xAI	Processing for requested AI operations, depending on the model actually used; entities and access countries under the relevant agreements. Google restrictions apply.
Apollo / ZenLeads, Inc.	Enrichment and matching on instructions in its role as processor; United States. Its own database involves a separate role and is not implicitly authorized by the DPA.
Tawk.to	Processing only when Customer data is transmitted to it for requested support; international access and transfers depending on the service.

Google, Microsoft, and the SMTP/IMAP provider directly selected by the Customer are also its connected services; their role depends on the operation and their agreement with the Customer. Stripe, Google Analytics, and the website's own processing are described in the Privacy Policy and are subprocessors under this DPA only when they actually process Customer data within this framework.

The list identifies authorized services without establishing that every provider receives every data category. Beeving documents the contractual entities, locations, safeguards, and actual recipients for each operation and provides that information to the Customer on request. Any addition follows Section 5.

Appendix 3. Technical and Organizational Measures

Area	Measures to Maintain
Transmission	TLS connections; secure mechanisms for communications and data return.
Secrets	Protection and encryption of OAuth tokens and email secrets at rest; restricted access; removal or rotation when no longer needed.
Access Control	Permissions by role and organization, production access restricted to authorized individuals, and review and removal of authorizations.
Separation and Minimization	Logical separation of customer data; limitation of fields, messages, and excerpts transmitted to providers.
Operations	Security maintenance and updates, appropriate monitoring, diagnostics, and vulnerability handling.
Traceability	Logs necessary for security and operational follow-up, with proportionate access and retention.
Backups	Protected copies, restricted access, controlled restoration; purge within a maximum of 90 days after account deletion.
Incidents	Assessment, containment, and notification process; operational contact and retention of relevant information.
Deletion and Rights	Return, correction, and deletion procedures; reapplication of deletion instructions after a restore; assistance with requests.
Personnel and Providers	Confidentiality obligations, appropriate awareness training, and contractual controls over access.

These measures are assessed in light of risk, the nature of the data, and the enabled service. They do not constitute ISO certification, a guarantee of infallibility, or a claim that a certification audit has been completed.

Appendix 4. Contacts and Acceptance

Party	Identification and Contact
Beeving / GROUPE GARAN	200 rue de la Croix Nivert, 75015 Paris, France; contact@beeving.com; +33 6 33 18 05 11.
Customer	Organization and representative stated in the order; address and contact information associated with the business account.
Customer Data Contact	Account administrator or data protection contact expressly communicated to Beeving.
Evidence of Acceptance	DPA version, relevant order, subscriber identity, and date of electronic acceptance, or a separately signed document.