

Privacy Policy

Personal Data Protection | Version dated October 13, 2026

1. Scope and Contact

This policy covers beeving.com, the app.beeving.com and dash.beeving.com applications, the APIs, and communications with Beeving. Personal data identifies a person directly or indirectly; pseudonymized data remains personal data.

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, determines the processing necessary to manage accounts, its business relationships, billing, support, security, and the operation of its website.

Contact for data and individual rights: contact@beeving.com. Phone: +33 6 33 18 05 11. The mailing address is GROUPE GARAN's registered office address.

2. Customer Data and Our Role as Processor

For imported or enriched contacts, campaigns, messages, replies, and CRM data processed solely on instructions, the customer determines the purposes and legal basis. Beeving acts as its processor, or as a subprocessor when the customer itself acts on another organization's behalf.

The DPA describes this processing, confidentiality, security, providers, assistance, and deletion. This policy does not replace the information that the customer must provide to its prospects, subscribers, or other contacts. A request concerning a campaign may be addressed to the sending customer; Beeving provides the required assistance.

3. Data Received and Sources

Category	Information and Sources
Account, team, and organization	Name, business email, company, role, invited users, permissions, subscription, and authentication data. Provided by you or your organization's administrator.
Contacts and CRM	Names, contact information, company, job title, lists, tags, custom fields, notes, sales stages, and interactions. Provided by the customer, its integrations, or Apollo when enrichment is requested.
Campaigns and messages	Content, templates, signatures, recipients, scheduling, sent messages, replies, necessary attachments, delivery events, objections, and statistics. Generated through usage and authorized email accounts.
Email connections	Account address, SMTP/IMAP settings, necessary secrets, OAuth tokens, and information accessible within the granted scope. Provided during setup or by Google/Microsoft.
AI and automation	Instructions, data excerpts, context, and results necessary for the requested generation, classification, or analysis. The scope depends on the feature used.
Billing and support	Billing details, invoices, transaction references, payment status, and support messages. Stripe processes payment data; Beeving does not retain full payment card numbers.
Usage and technical data	IP address, browser, device, login events, interactions, technical logs, and progress and badge data when used. Audience measurement through self-hosted Matomo and Google Analytics, subject to cookie choices.

Fields required for an account, payment, or a feature must be completed to use it. Optional data is identified as such. Do not send sensitive data, criminal-offense data, secrets, or information unrelated to the requested operation.

4. GROUPE GARAN's Purposes and Legal Bases

Purpose	Legal Basis
Account and subscription of an individual acting as a business owner	Contract performance or requested precontractual steps, GDPR Article 6(1)(b).
Users and contacts of a customer organization	Legitimate interest in providing the Service and managing the business relationship, Article 6(1)(f).
Billing and accounting obligations	Legal obligation, Article 6(1)(c), and contract performance when the person is a party to the contract.
Support and messages necessary for the Service	Contract performance, or legitimate interest in handling requests and maintaining the relationship with the organization.
Security, abuse prevention, and diagnostics	Legitimate interest in protecting users and infrastructure; legal obligation where applicable.
Audience measurement and optional features	Consent for nonexempt trackers and associated processing. Legitimate interest only where an exemption or the absence of a tracker subject to consent allows it.
Beeving marketing communications	Consent where required; legitimate interest for relevant business outreach, with information and a simple way to object.
Rights requests and requests from authorities	Compliance with a legal obligation.

For data processed for a customer, the customer determines the legal basis. Selecting an integration or granting OAuth authorization does not, by itself, constitute consent to every use of the data. Accepting the Terms of Sale and Use does not constitute consent to optional processing.

When relying on a legitimate interest, we limit processing to what is necessary and take individuals' rights and freedoms into account. Options for objecting are described in Section 12.

5. Google, Outlook, and SMTP/IMAP

Google and Microsoft Outlook connections enable authorized email operations: sending, reading the information necessary to process replies, synchronization, and campaign tracking. Depending on the feature, these operations concern message content and metadata and relevant attachments. The effective scope is the scope presented and authorized when connecting the account.

With a personal SMTP/IMAP setup, Beeving processes the necessary server settings and secrets. Access must be limited to what is needed. You may disconnect an email account or revoke

authorization through your provider; tokens that are no longer needed are revoked and deleted without waiting for an archive-retention period to expire.

The use and transfer of information received from Google APIs comply with the Google API Services User Data Policy and Google Workspace API User Data and Developer Policy, including the Limited Use requirements. Google data is not sold, transmitted to a data broker, used for advertising, or used to train general-purpose models.

Human access to Google data is limited to cases permitted by those policies, including your explicit agreement to support involving specific data, security, or a legal obligation. A general reference to Apollo or an AI provider does not authorize a transfer of Google data that conflicts with those restrictions.

Imported Google data that is no longer needed is deleted within thirty days after disconnection at the latest; corresponding backup copies are purged within ninety days at the latest. Data necessary for another lawful instruction is identified separately and remains subject to the applicable restrictions.

6. Enrichment with Apollo

At the customer's request, Beeving uses Apollo to supplement business data. Information necessary to match a contact is transmitted, and available data is returned to the Service. The customer must inform individuals of this indirect collection, its source, and its purposes in accordance with the GDPR.

Apollo is operated by ZenLeads, Inc. in the United States. It acts as a processor for some operations performed on instructions and as a separate controller for its own business contact database. These roles depend on the operation and contractual framework; naming Apollo therefore does not mean that it always acts solely on Beeving's behalf.

Contributing or reusing customer data for a provider's own database requires a lawful framework, appropriate information, and the required authorizations. It does not follow from the DPA's general authorization to engage subprocessors. Google data protected by Limited Use must not be supplied to a data broker.

Practices and rights relating to Apollo's own database are described at <https://www.apollo.io/privacy-policy> and <https://www.apollo.io/company/privacy-center>. For data held in Beeving, the customer remains responsible for honoring rights and objections, including during an update or further enrichment.

7. Artificial Intelligence and Profiling

Depending on the feature, data necessary for the operation is transmitted to OpenRouter and models from Anthropic, OpenAI, Google, or xAI. It may include instructions, message excerpts, contact data, or CRM information when required for the requested generation, analysis, or classification.

Results are used, in particular, to prepare content, organize replies, or help prioritize actions. This processing may constitute profiling when it evaluates individuals. The Service is not designed to make employment, credit, or other decisions on its own that produce legal or similarly significant effects; such uses require a specific framework.

Beeving does not authorize an independent purpose or training of general-purpose models solely because data is sent to perform a feature. The DPA governs processing on the customer's behalf. Rules specific to Google data continue to prevail.

Providers' retention periods and safeguards are not automatically the same as Beeving's. You may request relevant information about the model, recipients, retention, and safeguards associated with an operation at contact@beeving.com.

8. Recipients and Infrastructure

Service	Function and Scope
AWS	Hosting and application infrastructure in the European Union; safeguards and access governed by data protection agreements.
Cloudflare	Distribution and protection of the relevant website content and traffic. A global network that may involve access from outside the EEA.
OpenRouter; Anthropic; OpenAI; Google; xAI	AI routing and features for data necessary for the operation. International providers and access depending on the services used.
Apollo / ZenLeads, Inc.	Business contact enrichment; processor or separate controller depending on the operation, as explained in Section 6.
Google and Microsoft; selected SMTP/IMAP provider	Authentication and email within the granted permissions. Services selected by the customer also have their own contractual framework.
Stripe	Payments, billing, and fraud prevention; processor or separate controller depending on the operation.
Google Analytics; self-hosted Matomo	Audience measurement according to choices and exemption conditions. Self-hosted Matomo does not receive the data as an external SaaS provider.
Tawk.to	Support chat when used; messages and technical context relevant to the conversation.
Other authorized recipients	Authorized staff, the customer's authorized users, message recipients, and legally competent authorities.

Access is limited to people who need it and is subject to applicable confidentiality obligations. Beeving does not commercialize its customers' contact files. A provider's own processing, including Apollo's business database, is distinguished from processing performed solely on instructions.

In the event of a reorganization or transfer of the business, disclosures must respect the applicable purposes, rights, and restrictions; they do not create a general authorization for reuse.

9. Transfers Outside the EEA

Primary hosting in the European Union does not rule out all access from a third country. Apollo, OpenRouter, AI providers, Cloudflare, and other international services may involve transfers or access from outside the European Economic Area.

A transfer subject to GDPR Chapter V requires a valid mechanism: an adequacy decision that actually covers the recipient and processing, or appropriate safeguards such as standard contractual clauses accompanied by the necessary assessments and supplementary measures.

Transfers performed in our role as processor also comply with documented instructions and the DPA. You may obtain information and a copy of relevant safeguards at contact@beeving.com; secrets unrelated to the verification may be redacted. A provider's name alone does not prove that a certification or adequacy decision covers it.

10. Retention and Deletion

Data	Period or Rule
Account, CRM, contacts, campaigns, and messages under Beeving's control	During authorized processing and provision of the Service. After account deletion: production data erased within 30 days; backups within 90 days, measured from the same event.
Integration tokens and secrets	While needed for authorized access; removal, revocation, and deletion when no longer needed. Active tokens are not retained for a revoked connection.
Google data no longer needed after disconnection	Production: a maximum of 30 days after disconnection; backups: a maximum of 90 days, as described in Section 5.
Mandatory invoices and accounting records	10 years for records covered by Article L123-22 of the French Commercial Code, with restricted access and use limited to the obligation.
Support and account-related logs	Time necessary to handle the request, diagnose issues, or ensure security; after deletion, 30 / 90-day limits, except where retention is legally necessary and documented.
Objections to a customer's campaigns	Minimum information according to the customer's instructions to prevent further solicitation. After processing ends, the customer receives the necessary data and Beeving applies the DPA's rules.
Cookies and audience measurement	Service-specific periods stated in the preferences module and Cookie Policy. Acceptance and rejection are remembered for six months under the selected setup.

Canceling a subscription does not, by itself, constitute a request for immediate erasure. The customer may request return of data or account closure at contact@beeving.com; any applicable retrieval period is taken into account before deletion starts.

Backups awaiting purge are protected, isolated from routine use, and subject to deletion instructions if restored. Retention required by law or necessary for an identified dispute is limited, documented, and segregated; it does not permit outreach to resume.

Beeving's retention period does not delete copies held by recipients or providers acting for their own purposes. For subprocessors, deletion and return are governed by the DPA and the relevant agreements.

11. Cookies, Email Pixels, and Security

Trackers that are not strictly necessary or exempt are blocked until the corresponding agreement is given. You may reject, customize, and withdraw your agreement through the cookie management module. Self-hosted Matomo is not automatically exempt; Google Analytics requires consent under the selected setup.

Campaign open or click tracking is separate from website cookies. The sending customer must inform recipients and comply with the applicable consent or exemption rules. Authorization for outreach does not constitute general authorization for tracking.

Security measures include, in particular, encrypted connections, protection of secrets and access tokens, limits on permissions and production access, and backup and incident management. They are adapted to risk and do not constitute a promise of zero risk. Measures applicable to customer data are set out in the DPA.

12. Your Rights

Depending on the processing and statutory conditions, you may request access, correction, erasure, restriction, and portability of data you provided when automated processing is based on your consent or a contract. You may withdraw consent for future processing.

You may object to processing based on a legitimate interest for reasons relating to your particular situation. You may object to marketing at any time without giving a reason. Requests may be sent to contact@beeving.com or GROUPE GARAN's registered office.

We respond within one month of receipt at the latest. If requests are complex or numerous, this period may be extended by two months, with notice and reasons provided within the first month. Exercising rights is generally free. Identity verification must remain necessary and proportionate; identification documents are not routinely required.

For campaign or CRM data belonging to a customer, we forward the request to the relevant controller and assist it under the DPA. We remain directly responsible for responses concerning our own processing.

You may lodge a complaint with the CNIL at <https://www.cnil.fr/fr/adresser-une-plainte>, or another competent supervisory authority. This right does not depend on first submitting a complaint to Beeving.

13. Business Users and Updates

The Service is reserved for adult business subscribers. It is not intended to collect minors' data for campaigns. Report any inappropriate situation to contact@beeving.com.

A significant change to this policy is announced by email or within the Service. It does not replace consent required for a new purpose. The date of this version appears on the first page.



14. Information About Third-Party Services

Google: <https://policies.google.com/privacy>; Google policies: <https://developers.google.com/terms/api-services-user-data-policy> and <https://developers.google.com/workspace/workspace-api-user-data-developer-policy>.

Apollo: <https://www.apollo.io/privacy-policy>; OpenRouter: <https://openrouter.ai/privacy>; Stripe: <https://stripe.com/privacy>; Tawk.to: <https://www.tawk.to/privacy-policy/>.

These links provide additional transparency about providers. They do not replace Beeving's own obligations or the customer's obligations.