

Data Processing Addendum

Version 1.0, effective 19 October 2026

Parties

Controller: the customer who has accepted the Terms ("Controller", "you").

Processor: Rosel Group LTD, 10 Kishinev Street, floor 4, apt. 28, Lozenets district, 1407 Sofia, Bulgaria, registered in the Bulgarian Commercial Register under UIC/EIK 206801487, VAT BG206801487, operating the Emporiqa service ("Emporiqa", "Processor", "we").

This Data Processing Addendum ("DPA") forms part of the Emporiqa Terms of Service at <https://emporiqa.com/terms-of-service/> (the "Terms") and governs our processing of personal data on your behalf under Article 28 of Regulation (EU) 2016/679 ("GDPR"). It applies automatically when you accept the Terms, which is the written form, including electronic form, that Article 28(9) GDPR requires. No signature is needed. If you want a signed copy for your records, download the signed PDF from <https://emporiqa.com/dpa/>, add your company details and signature, and keep it.

1. Subject matter, roles and duration

- 1.1 We provide an AI chat for your online store (the "Service"). When the chat runs on your store, you are the controller of the personal data of your store's visitors and customers, and we process it as your processor.
- 1.2 We are controller, not processor, of the data we need to run our own business: your account and team members' sign-in data, billing records, and our server and security logs, which contain your visitors' IP addresses. Our Privacy Policy at <https://emporiqa.com/privacy-policy/> covers that data.
- 1.3 The nature, purpose, categories of data and data subjects, and retention periods are set out in Annex I.
- 1.4 This DPA applies for as long as we process personal data on your behalf, and ends when that data has been deleted under section 11.

2. Your instructions

- 2.1 We process personal data only on your documented instructions, including with regard to transfers to third countries. Your instructions are the Terms, this DPA, and the settings you choose for your store in the Emporiqa dashboard and in our plugin (for example voice mode, photos, page context, recognition of signed-in customers, store rules, order linking and Load on click).
- 2.2 You give further instructions in text form, by email from the account owner to support@emporiqa.com. We confirm oral instructions in text form.
- 2.3 We tell you without undue delay if we believe an instruction infringes the GDPR or other Union or Member State data protection law, and we may suspend that instruction until you confirm or change it.
- 2.4 We process personal data otherwise only where Union or Member State law requires it. In that case we tell you before processing, unless that law prohibits it on important grounds of public interest.

3. Confidentiality

Everyone we authorise to process the personal data is bound to confidentiality, by contract or by a statutory duty.

4. Security

4.1 We implement the technical and organisational measures in Annex II, and we keep them at a level appropriate to the risk (Article 32 GDPR).

4.2 We review these measures regularly and may change them as technology develops, provided the overall level of protection does not decrease.

5. Sub-processors

5.1 You give us general written authorisation to engage the sub-processors listed in Annex III and at <https://emporiqa.com/subprocessors/>.

5.2 We will notify you by email at least 30 days before we engage a new sub-processor that processes your personal data, or replace an existing one. You may object within that period on reasonable data protection grounds. If we cannot address the objection, you may terminate the Service for the affected store without charge before the change takes effect.

5.3 We impose on each sub-processor, by contract, the same data protection obligations as set out in this DPA (Article 28(4) GDPR). Where a sub-processor offers audit reports or certifications instead of audits, we rely on those and pass them to you on request. We remain fully liable to you for each sub-processor's performance of its obligations.

5.4 Where you send data to Slack, Microsoft Teams, Discord, Google Chat, Zapier, Make or your own endpoints through store alerts or store rules, those are your recipients, not our sub-processors. We send to them on your instructions; their terms and any transfer basis are your responsibility.

6. International transfers

6.1 We store and process personal data on servers in Germany, rented from Hetzner Online GmbH. Some sub-processors in Annex III process personal data outside the European Economic Area.

6.2 For each such transfer we rely on the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), Module 3 (processor to processor), and on the EU-U.S. Data Privacy Framework where the sub-processor is certified under it.

6.3 If you are established outside the EEA, Module 4 (processor to controller) of those clauses applies to our transfers of personal data to you, to the extent the GDPR requires it.

6.4 If a public authority asks us for your personal data, we tell you before we disclose anything, unless the law prohibits it, and we disclose only what the law requires.

7. Assistance

7.1 **Data subject requests.** If a data subject contacts us directly, we forward the request to you without undue delay and do not answer it ourselves unless you ask us to. On your written request we delete, or give you a copy of, the conversations of a data subject you identify, within 10 working days. There is no self-service delete or export function in the dashboard yet; we do this for you.

7.2 **Impact assessments and consultations.** We give you the information you reasonably need for a data protection impact assessment or a prior consultation with a supervisory authority, as far as it concerns our processing.

7.3 **Supervisory authorities.** We cooperate with the supervisory authorities in the performance of their tasks (Article 31 GDPR).

8. Personal data breaches

8.1 We notify you without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting your personal data.

8.2 The notice describes, as far as we know at the time, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed. We provide further information in phases as it becomes available.

8.3 Notifying you is not an acknowledgement of fault or liability.

9. Records and contact

9.1 We keep a record of the processing we carry out on your behalf (Article 30(2) GDPR).

9.2 We have not appointed a data protection officer, as we are not required to. Data protection questions go to support@emporiqa.com, answered by Rosen Hristov, founder of Emporiqa.

10. Audits

10.1 We make available all information necessary to demonstrate compliance with Article 28 GDPR, including this DPA and its annexes, our sub-processor list, and written answers to your reasonable security and privacy questions.

10.2 If that information is not sufficient, we allow for and contribute to audits, including inspections, by you or an independent auditor bound by confidentiality: once in any 12 months, with at least 30 days' notice, during business hours, without access to other customers' data, and at your own cost. These limits do not apply where a supervisory authority requires the audit or after a personal data breach affecting your data.

10.3 We hold no ISO 27001 or SOC 2 certification at the date of this DPA.

11. Deletion and return

11.1 When you close a store, or the Terms end, we delete the store and its personal data 30 days after the closure. You can cancel a closure within those 30 days.

11.2 Before deletion, you may ask us for a copy of the conversations of that store in a common machine-readable format, such as JSON.

11.3 We keep the 30 most recent nightly backups, all encrypted, and the backup storage keeps 10 daily snapshots of them. Deleted data leaves them as newer backups and snapshots replace them, normally within six weeks, and later if backups pause.

11.4 On request, we confirm the deletion in text form.

11.5 We do not keep the personal data after that, unless Union or Member State law requires us to store it.

12. Liability and precedence

12.1 Each party's liability under this DPA is subject to the limitations in the Terms, except that those limitations do not apply to liability for breaches of this DPA caused by intent or gross negligence, to the parties' recourse under Article 82(5) GDPR, or where the law does not allow them to be limited.

12.2 If this DPA and the Terms conflict on the processing of personal data, this DPA prevails. If the Standard Contractual Clauses apply and conflict with this DPA, the clauses prevail.

13. Changes to this DPA

13.1 We may update this DPA. We give you at least 30 days' notice by email before a change that affects your rights takes effect. A change never lowers the protection of your personal data under this DPA.

13.2 The current version is published at <https://emporiqa.com/dpa/>. Earlier versions are available on request.

14. Governing law and language

14.1 This DPA is governed by the laws of the Republic of Bulgaria, and the courts of Sofia, Bulgaria have jurisdiction, as in the Terms. This does not affect any rights data subjects have under the GDPR.

14.2 This DPA is published in English, and the English text governs.

Annex I: Description of the processing

Data subjects

- Visitors to your store who open or use the chat, and, in the default loading mode, visitors whose browser loads the chat.
- Your customers, where they use the chat or are signed in to your store.
- Every customer who places an order in your store while order linking is on, whether or not they used the chat. In the Shopware plugin this is the "Link orders to chats" switch; our other plugins send orders whenever they are connected.
- Members of your team, as far as they appear in conversations they take over.

Categories of personal data

Data	When	Kept
Chat messages and anything a visitor writes in them, including contact details they give	Every conversation	Until 90 days after the conversation's last activity
Visitor's country (from Cloudflare) and language	Every conversation	As the conversation
Page context: the address and title of the page the visitor is on, and recently viewed products	On by default. With Load on click, after the click: only the page the visitor is on, no recently viewed products	As the conversation; sent to the AI model with the message
Transcripts of spoken messages	Voice mode on (off by default)	As chat messages
Voice recordings of spoken messages	Voice mode on	Not stored by us; sent to OpenAI to be transcribed
Spoken replies (audio)	Voice mode on	Up to 5 minutes, for playback
Photos a visitor sends	Photos allowed (store setting)	7 days. EXIF and GPS data are removed before the photo is described by OpenAI or stored by us
Photos your team attaches to a reply	Team takeover	90 days from upload, or earlier if the conversation is deleted
Keyed hash (HMAC) of the visitor's connection, for rate limits and blocking	Every conversation	As the conversation

Data	When	Kept
Server-side usage fingerprint (hash of IP address, browser, store and a daily salt)	Default mode only; not computed with Load on click	Daily counts; cannot link a visitor across days
Signed customer id and customer-specific prices	"Recognise signed-in customers" on (default on), signed-in customers only, never guests	As the conversation; prices read from your store are cached 5 minutes
Customer's first name	Greeting a signed-in customer	Stored in the greeting reply, as the conversation
Customer account name, email and newest order	Handoff to your team, or a store rule that asks for them	Cached up to 30 minutes; what is passed to your team stays with the conversation
Order details your store returns for an order lookup (order number, names, contents, status, delivery details)	"Order status" rule on, after the visitor gives order number and order email, or is signed in	As the conversation; sent to the AI model to write the answer
Order records: order number, total, currency, items and the conversation id (no name, email or address, unless your developers extend the payload)	Order linking on	90 days; an order linked to a conversation is deleted with that conversation
Handoff records: AI summary of the conversation, your team's notes and resolution notes	Handoff to your team	As the conversation
Rule records (field names, outcomes, masked excerpts) and the details a rule sends to your team	Store rules you set up	As the conversation; emails waiting for delivery up to 2 days
English translation of a message for a team email	Team emails in another language	7 days
Chat block list entries (customer id or connection hash, and the reason your team gives)	When your team blocks a visitor	Customer blocks until your team removes them. Connection blocks stop applying after 90 days; the expired entry stays in the block list until your team removes it or the store is deleted
Chat ratings and the reason given	When a visitor rates a chat	As the conversation
Catalogue and page data your store sends that contains personal data, if any	Store sync	While the store is active; held back for up to 30 days if a sync batch is rejected

We do not ask for special categories of personal data (Article 9 GDPR). A visitor can type them into the chat; we process them only as part of the conversation.

Store alerts to Slack, Microsoft Teams, Discord and Google Chat include the visitor's question, up to 150 characters. Email alerts and digests of unanswered questions include it in full. These go to the recipients you set up (section 5.4).

Data on the visitor's device

- **Load on click** (two-click solution): before the visitor clicks your store's own chat button, the browser makes no request to us and nothing is written to cookies or browser storage. The button reads one localStorage entry, `emporiqaChatOpened_<store id>`, which exists only if this visitor opened the chat before. It is written when the visitor opens the chat, is acted on for 30 days, and stays until site data is cleared. After the click, the chat writes the storage entries it needs to run.
- **Default mode:** the browser storage entries are written when the page loads.
- **emporiqa_sid cookie:** first party, 1 hour sliding, SameSite=Lax, Secure on https, links an order to the conversation. Not set when order linking is off.

The full list per mode, with lifetimes, is at <https://emporiqa.com/cookies/> and <https://emporiqa.com/docs/widget-embedding/#load-on-click>.

Nature and purpose

Running the chat on your store: answering visitors' questions from your catalogue and pages, product search (including from a photo), comparing products, adding to cart, order status, store rules, handing conversations over to your team, voice input and output where you switch it on, showing you conversations and analytics in the dashboard, linking orders to chats, and protecting the Service against abuse.

Retention of other copies

- OpenAI keeps API requests for up to 30 days for abuse monitoring and does not use them for training. We have applied for zero data retention.
- Our cache keeps rule-matching answers for 10 minutes.
- Backups: see section 11.3.

Frequency

Continuous, for as long as the chat runs on your store.

Annex II: Technical and organisational measures

Physical access control

Our servers run in Hetzner data centres in Germany, which hold ISO/IEC 27001 certification. We have no physical access to them; Hetzner controls entry to the buildings.

System access control

Servers are reached only over SSH with a key, by one named person (the founder of Emporiqa); password login is disabled. Our administration interface requires a Google sign-in. Your team signs in to the dashboard with a one-time email link, Google, Microsoft or GitHub, or a password they set; sessions use Secure and HttpOnly cookies. Two-factor sign-in for the dashboard is not available yet; a team member who signs in with Google, Microsoft or GitHub gets that provider's two-factor protection.

Data access control

Each team member sees only the stores they belong to. Our own staff can open a store's dashboard read-only through an administrator function that requires Google sign-in; we use it only for support or to carry out your instructions. Photos are served only through access-checked views, to your team and to the visitor in their own conversation. Filenames are random.

Transfer control

TLS 1.2 or higher for all public traffic (chat widget, dashboard, API) and for all transfers to sub-processors. Requests between your store's plugin and us are signed with HMAC-SHA256 in both directions. Signed customer tokens expire after 7 days. Order lookups require the order number and order email, or a signed customer id. Error reports sent to Sentry are filtered to remove chat message bodies and form data.

Input control

Messages from your team are recorded with the team member who sent them. Changes to a store's rules are kept in a history. Account activity is logged and kept 2 years.

Order control

Sub-processors are bound by contract under section 5.3. Personal data sent to AI model providers is not used to train models. Voice recordings are not stored by us and are not used to identify a speaker; no voiceprints are created.

Availability control

Nightly backups go off-site to a separate Hetzner Storage Box in Germany, reachable only by SSH key, are checked with SHA-256 after upload, and are monitored for missed runs. The Storage Box also keeps 10 daily snapshots, which the production server cannot change or delete. Restoring from a backup is tested.

Separation control

Every record is scoped to its store, including the search index.

Encryption

Nightly backups are encrypted with age (public-key encryption) before they leave the server; the servers hold only the public keys, so neither the production server nor the backup storage can read a backup. A backup that cannot be encrypted is not uploaded. Webhook signing secrets and the Slack, Microsoft Teams, Discord, Google Chat and rule webhook addresses you configure are encrypted with Fernet. The databases and server disks are not encrypted at rest; they are protected by the access controls above.

Abuse protection

Sending messages, uploading photos and voice, order lookups, ratings and the plugin webhooks are rate limited per connection across several time windows. The visitor's connection is stored with a conversation only as a keyed hash. Raw IP addresses are held in rate-limit counters for up to 24 hours and in the web server's access log, a fixed-size buffer that at current traffic holds less than a day. Our application logs do not record IP addresses.

Data minimisation

Load on click keeps all requests and storage until the visitor asks for the chat. Order records carry no name, email or address. For the greeting, a signed-in customer's first name is put into the reply after the AI model has written it, so it is not sent to the model for that purpose. A visitor's photo has its EXIF and GPS data removed before it is described by the AI model or stored. Optional features (voice mode, photos, page context, recognition of signed-in customers, order lookups, order linking) can each be switched off.

Retention

Scheduled jobs delete conversations 90 days after their last activity, photos sent by visitors after 7 days, order records after 90 days, and activity logs and usage analytics after 2 years.

Review

Changes to the platform pass an automated test suite before release. We review these measures when the Service changes and at least once a year. Incidents are handled and notified under section 8.

Certification

None at the date of this DPA (no ISO 27001, no SOC 2).

Annex III: Sub-processors

Sub-processor	Purpose	Personal data	Location	Transfer basis
OpenAI Ireland Ltd	AI model: chat replies, embeddings, describing photos, transcribing voice, spoken replies	Chat messages and page context, photos, voice recordings, and details a visitor gives for order lookups and store rules, with your store's answer	Ireland; processed in the United States by OpenAI's affiliates	EEA contract; OpenAI's onward transfers to the United States under SCCs
OpenRouter, Inc.	Search result reranking with the Cohere Rerank model; OpenRouter passes the request to Cohere, the model's provider, which does not use it for training	The visitor's search query, with product and page text. OpenRouter does not keep it (prompt logging off); Cohere keeps it under its own terms, not zero retention	United States	SCCs in OpenRouter's data processing agreement, part of its terms
Cloudflare, Inc.	CDN, TLS, DDoS protection, edge caching of the team photos shown in the chat, bot check when shown	IP addresses, request metadata, traffic in transit, cached team photos, Turnstile browser signals	United States (global edge network)	SCCs Module 3
Functional Software, Inc. (Sentry)	Error tracking	Stack traces, request metadata, platform user identifiers and a hashed IP address; filtered to remove chat message bodies	United States	SCCs Module 3
Sendinblue SAS, trading as Brevo	Sending handoff alerts, rule emails and digests to your team	Recipient addresses, email content, contact details and messages from the conversation	France	EEA
Hetzner Online GmbH	Servers, databases, file storage, backups	All stored data	Germany	EEA

Where a sub-processor is also certified under the EU-U.S. Data Privacy Framework, that certification applies in addition.

Stripe, Inc. and Stripe Payments Europe, Ltd. process your account and billing data, for which we are controller (section 1.2), not visitor data. They appear on our public sub-processor list for completeness.

The current list is at <https://emporiqa.com/subprocessors/>.

Signatures

Controller

Company

Name

Title

Date

Signature

Processor

Company

Rosel Group LTD

Name

Elena Samardzhieva

Title

Managing Director

Date

19 October 2026

Signature

