

Privacy Policy

Version 1.1. Last updated: 16 October 2026. Czech version: /cs/privacy. If the two versions differ, the Czech text prevails.

This policy explains how Stockbird s.r.o. handles personal data. It applies to our website stockbird.app, our web and device applications, and our business communications.

1. Who we are

Stockbird s.r.o., company ID (IČO) 29976669, registered office Bezručova 4201, 430 03 Chomutov, Czech Republic, registered in the commercial register kept by the Regional Court in Ústí nad Labem, section C, file number 56422. We are not a VAT payer.

Contact for all privacy matters: info@stockbird.app.

We have not appointed a data protection officer because Article 37 GDPR does not require one for our activities. The contact above handles all privacy requests.

2. Two roles: controller and processor

Stockbird acts in two different roles, and your rights depend on which one applies.

- As a controller we decide why and how personal data is used. This covers visitors to our website, people who book a demo, newsletter subscribers, account holders and administrators of our applications, and billing contacts of our customers.
- As a processor we handle data on behalf of our customers (restaurants and food-service businesses) who use Stockbird to run their operations. The customer is the controller of that data, and we process it only on the customer's documented instructions under a data processing agreement (DPA). This covers business data customers load into Stockbird, including names, phone numbers and email addresses of their staff, uploaded documents and operational records.

If you are an employee or contact of one of our customers and want to exercise your rights over data held in the customer's Stockbird account, please contact the customer first. If you write to us, we will forward your request to the customer and help them answer it.

3. What data we process, why, and on what legal basis

Who	Data	Purpose	Legal basis (GDPR)	Retention
Website visitors	IP address, request logs, browser and device metadata	Serving and securing the website, rate limiting of forms	Legitimate interest, Art. 6(1)(f): secure and reliable service	Server logs: 30 days. Rate-limit keys: transient, minutes to hours
Website visitors and product users	Pseudonymous usage events keyed to internal identifiers, error traces, feature-flag evaluations, IP and browser metadata	Product analytics, stability and improvement. Cookieless: no analytics cookies or persistent browser identifiers are set	Legitimate interest, Art. 6(1)(f)	Up to 12 months
People who book a demo	Name, email address, company, meeting details	Scheduling and conducting the demo, answering your enquiry	Steps at your request before a contract, Art. 6(1)(b); legitimate interest in answering business enquiries	Until the enquiry is resolved, then up to 24 months if no contract follows
Account holders and admin dashboard users	Name, email address, credentials and session tokens, organisation membership, usage records	Providing the service, authentication, security, support	Contract, Art. 6(1)(b)	Duration of the contract, then deleted within 30 days of termination; backups roll off afterwards

PRIVACY POLICY — EN

Customers' billing contacts	Name, email, company, invoicing address, subscription and invoice records. Card details are handled by Stripe and never stored by us	Billing, payments, collecting receivables	Contract, Art. 6(1)(b); legal obligation, Art. 6(1)(c)	Invoices and accounting records: 5 to 10 years depending on document type, as required by Czech accounting and tax law
Newsletter subscribers	Name, business email address, company, role, record of your consent	Newsletter and product news	Consent, Art. 6(1)(a), requested separately from any contract, and Act 480/2004 Coll. §7	Until you withdraw consent or unsubscribe; we keep a record of the consent as proof
Anyone who contacts us	Email content, attachments, contact details	Answering your message and keeping a record of business correspondence	Legitimate interest, Art. 6(1)(f)	Up to 3 years after the last contact

We send our newsletter and similar marketing emails only if you have given us separate, voluntary consent. Giving or refusing that consent has no effect on your use of Stockbird. You can withdraw it at any time using the unsubscribe link in every email or by writing to us.

We do not knowingly collect special-category data, and our service is not directed at children. We do not sell personal data.

4. Data we process as a processor for customers

Customers use Stockbird to manage their operations, so their Stockbird account may contain:

- names, phone numbers and email addresses of their staff;
- shift records created by staff using the Stockbird device app, which identifies a device and does not use a personal login;
- documents and attachments the customer uploads, such as pay-related documents;
- messages exchanged through channels the customer chooses to connect, for example a Telegram bot, and data from point-of-sale or supplier systems the customer connects.

We use this data only to provide the service to that customer. We never use customer data for our own purposes, and we never use it to train AI models. Retention follows the customer's instructions. On termination we delete customer data within 30 days and our backups expire within a further 35 days.

Channels and systems the customer chooses to connect (such as Telegram or a point-of-sale system) are the customer's own vendors. They are not subprocessors engaged by Stockbird, and their own privacy terms apply.

5. Artificial intelligence features

Some Stockbird features use large language models to answer questions or analyse the customer's business data. Prompts and outputs are sent through an AI gateway operated by Requesty Ltd, and we use only models hosted in the European Union. Requesty stores data in Frankfurt, Germany. We record prompts, outputs and evaluations in an EU-hosted observability tool (Langfuse) to monitor quality and fix errors. Customer data is not used to train models, under our contracts with these providers. No decision with legal or similarly significant effect on an individual is made solely by automated means.

6. Recipients and subprocessors

We share personal data only with service providers that need it, under written agreements that meet Article 28 GDPR. The table lists everything we use that can touch personal data. We will give customers at least 30 days' notice before adding a new subprocessor, with a right to object.

PRIVACY POLICY — EN

Provider	What it does for us	Data	Location	Transfer safeguard
Hetzner Online GmbH	Server hosting for our applications and background jobs	All application data, server logs	Germany (Nuremberg)	None needed: EU/EEA only
Neon, Inc. (Databricks)	Managed PostgreSQL database	Customer accounts and business data	EU region	EU-US Data Privacy Framework (DPF); SCCs and UK Addendum as fallback
Cloudflare, Inc. (Cloudflare Germany GmbH)	DNS, content delivery and security proxy; file storage	IP addresses and request metadata; uploaded files	Global edge network; file storage in the EU	DPF; SCCs as fallback
Requesty Ltd (UK)	AI gateway to language models	Prompts and outputs, which may contain customer business data	Frankfurt, Germany; EU-hosted models only	None needed with EU endpoint and EU-hosted models; SCCs and UK Addendum as fallback
Langfuse GmbH	AI quality monitoring and tracing	Prompts, outputs, traces, evaluations	EU (Langfuse EU Cloud)	None needed by default; SCCs and/or DPF for any access from outside the EEA
Clerk, Inc.	Sign-in and identity for our applications	Email, name, credentials, session tokens, organisation membership	United States	DPF; SCCs and UK/Swiss addenda as fallback
Resend, Inc.	Sending service and notification emails	Recipient name and email address, message content, delivery metadata	EU region	DPF; SCCs and UK Addendum as fallback
PostHog, Inc.	Product analytics, error capture, feature flags	Pseudonymous usage events, error traces, logs, browser and IP metadata	EU (PostHog EU Cloud)	DPF; SCCs and UK Addendum as fallback
Vercel Inc.	Hosting of our web front ends	Visitor IP addresses, request logs	Global edge network	SCCs and UK Addendum
Upstash, Inc.	Rate limiting of website forms	IP addresses, transient	EU region	DPF; SCCs and UK Addendum as fallback
Calendly LLC	Demo scheduling. The widget loads only when you choose to book	Name, email address, meeting details	United States	DPF; SCCs and UK Addendum as fallback
Stripe Payments Europe, Ltd (Ireland); Stripe, Inc.	Subscription billing and payment processing. Stripe also acts as an independent controller for fraud prevention and legal compliance	Billing contact, invoicing address, payment details, invoices	EU and United States	DPF; SCCs
Crisp IM SAS	Knowledge base, help center, and customer support chat (widget and inbox)	Visitor and user names, email addresses, company, chat messages, IP addresses, devices, session cookies, website information, knowledge-base interactions	France (Nantes), 2 boulevard de Launay, 44100 Nantes	None needed: EU/EEA only

Other recipients, in their own right: our email and document provider (Google Workspace) for business correspondence; banks and payment institutions for legal and financial obligations; professional advisers; and public authorities where the law requires disclosure.

7. International transfers

Where a provider is located outside the EU/EEA (for example in the United States), we rely on the European Commission's adequacy decision for the EU-US Data Privacy Framework where the provider is certified, and otherwise on the Standard Contractual Clauses (Commission Decision 2021/914) with supplementary measures. Requesty is based in the United Kingdom, which benefits from an EU adequacy decision, and its contract also incorporates Standard Contractual Clauses. You can ask us for a copy of the safeguards at

info@stockbird.app.

8. Cookies and similar technologies

We do not use advertising cookies, and our product analytics runs in cookieless mode, so we do not set analytics cookies or persistent identifiers on your browser. We use only strictly necessary technologies, for example session cookies set by our sign-in provider so you can log in to the application. Under §89(3) of Act 127/2005 Coll. these do not require consent. If we add non-essential cookies in the future, we will ask for your consent first and update this section.

9. Security

We protect personal data with measures appropriate to the risk, including encryption in transit, hosting in certified data centres (ISO 27001) in the EU, access limited to named personnel on a need-to-know basis, separation of production and development data, and written data protection agreements with every provider. We will notify the supervisory authority and affected parties of a personal data breach where the law requires.

10. Your rights

Under GDPR you have the right to:

- access your data and receive a copy (Art. 15);
- have inaccurate data corrected (Art. 16);
- have data erased (Art. 17);
- restrict processing (Art. 18);
- receive your data in a portable format (Art. 20);
- object to processing based on legitimate interest, and to direct marketing at any time (Art. 21);
- withdraw consent at any time, without affecting earlier processing (Art. 7(3)).

Email info@stockbird.app. We answer within one month and may need to verify your identity. Every marketing email contains an unsubscribe link. You may also lodge a complaint with the Czech supervisory authority: Úřad pro ochranu osobních údajů (ÚOOÚ), Pplk. Sochora 27, 170 00 Praha 7, www.uoou.gov.cz, or with the authority in your own EU country.

11. Is providing data mandatory?

Providing data is voluntary except where needed to create an account, sign a contract or meet our legal obligations. Without it we cannot provide the related service.

12. Changes to this policy

We will post updates on this page with a new date and version. For material changes affecting customers, we will notify account administrators by email.