

Privacy Notice

Version 5 September 2026

Information about Passvanta's processing of personal data.

Controller and privacy contact

The controller under the General Data Protection Regulation is Ömer Salmaz, Passvanta, Philippsburger Straße 83a, 68753 Waghäusel, Germany. Send privacy requests to privacy@passvanta.com. Passvanta has not appointed a data protection officer. If a statutory appointment duty arises, this notice will be updated.

Scope and roles

This notice covers the public websites, the Passvanta application, customer accounts, Supplier guest links and Supplier accounts, and the contact, demo, Readiness Check and file-upload functions.

Passvanta is controller for its website, pre-contract communications, customer management, billing, security, support and marketing. Where business customers place personal data of employees, suppliers, contacts or other persons in Passvanta and determine the purposes and means, Passvanta generally processes that data as processor. An Article 28 GDPR data processing agreement must apply before such processing starts.

Customers may authorise members of a Supplier or Service Provider organisation for specific organisations, products, requests or data fields. The Customer determines the purpose and scope of the disclosure and remains responsible for its lawfulness. Passvanta implements the permission, separates tenants and logs security- and compliance-relevant grants. A Service Provider receives no general access to other Customer organisations.

Server access, hosting and security

When a person uses the website or app, technically necessary connection data is processed. This may include IP address, date and time, requested URL, referrer, browser and device information, response status, security events and technical identifiers. The purposes are delivery, stability, troubleshooting and prevention of attacks. The legal basis is Article 6(1)(f) GDPR and, for contractual use, Article 6(1)(b) GDPR. Passvanta's legitimate interest is the secure and reliable operation of the service.

Vercel hosts web and application components. Because Passvanta is commercial, it must not use Vercel's Hobby plan; a paid Pro or Enterprise plan with voluntary model-training use disabled is required. Cloudflare provides DNS, CDN, web application firewall and security services. IONOS is used only for domain registration and email-address administration. The operational database uses the Neon Platform. For third-country processing, Passvanta relies on the safeguards in the relevant provider DPA, particularly Standard Contractual Clauses or an applicable adequacy decision. Database and AI regions must be configured and documented in the relevant accounts.

Security logs are generally retained for up to 30 days. Data required to investigate a specific incident may be retained until the investigation is complete and thereafter for applicable limitation or evidence periods.

Contact, demo and Readiness Check

For contact and demo requests, Passvanta processes the name, business contact details, company, message, scheduling preferences and technical metadata. The legal basis is Article 6(1)(b) GDPR where the request concerns a contract, and otherwise Article 6(1)(f) GDPR. Non-contractual requests are normally deleted no later than twelve months after closure, subject to legal retention duties.

The DPP Readiness Check processes product and company information, answers, result data and technical metadata to provide the requested result. Without an account, personal inputs and linked uploads are generally deleted after 30 days. With an account, they are stored as Customer Content under the contract and customer

settings. The legal basis is Article 6(1)(b) GDPR for requested pre-contract or contractual use, and otherwise Article 6(1)(f) GDPR.

File uploads and product data

Upload functions may process documents, product data, supplier evidence and personal data contained in those materials. Users may upload only data for which they have a lawful basis and disclosure right. Special-category data under Article 9 GDPR, criminal-conviction data under Article 10 GDPR, private identity documents and complete payment credentials are not intended for Passvanta and must not be uploaded unless expressly approved by contract and privacy review in advance.

Files uploaded without an account are generally deleted after 30 days. For customer accounts, storage follows the contract, deletion functions and legal duties. After contract termination, exportable data remains retrievable for at least 30 calendar days unless earlier deletion is instructed. Customer Content is then deleted or anonymised, subject to necessary backup cycles and legal obligations.

Under the confirmed operating model, uploads and related metadata are stored in the Neon database. If Passvanta later introduces separate object or file storage, that provider must be added to this notice and the DPA before first use and reviewed for region, deletion, backup and international transfer.

Public DPPs and data sharing

A Customer may instruct Passvanta to make selected product-passport data public or share it with specified recipients. Publicly marked content can be accessed worldwide without signing in and may be further processed by search engines or third parties. Before publication, the Customer must review permissions, trade secrets and the necessity of any personal data. Personal data must not be published merely because it appears in evidence or a DPP field.

Passvanta processes publication, withdrawal, version, approving person and related audit data for contract performance and security. Access and security logs for public DPP pages are generally retained for up to 30 days. Technical publication or registry transmission is not approval by an authority.

Accounts and Passvanta authentication

For customer and Supplier accounts, Passvanta processes name, business email address, password hash, organisation, roles, permissions, invitation status, session data, sign-in times, security events and audit records. Plain-text passwords are not stored. The legal basis is Article 6(1)(b) GDPR, with Article 6(1)(f) GDPR additionally supporting security logs. Account data is stored for the contract term. Security and audit data is restricted under a documented deletion policy.

Supplier guest links use a random, time-limited and revocable access token. Recipients must not share the link. Passvanta may require an additional email verification for sensitive requests.

Contract, billing and Stripe

For subscriptions, billing and payment, Passvanta processes company and contact data, billing address, plan, service period, amount, payment status, transaction identifier and tax data. Passvanta issues its own invoices and sends them through Resend. Stripe processes payment credentials; Passvanta does not store full card or bank details where Stripe tokenises the payment.

For a German Stripe account, the contracting entity is generally Stripe Payments Europe, Limited, Ireland. Depending on the function, Stripe acts as processor and as an independent controller, including for fraud prevention and its own legal duties. The legal bases are Article 6(1)(b), (c) and (f) GDPR. Accounting vouchers are generally retained for eight years and business correspondence for six years, with longer storage where required by tax law.

Email and newsletter

All transaction, invitation, support, billing and newsletter email is sent through Resend, Plus Five Five, Inc., United States. The service processes sender and recipient address, subject, content, delivery status and technical metadata. Depending on the message, the legal basis is Article 6(1)(b), (c) or (f) GDPR. Resend's DPA incorporates the SCCs and states that the provider participates in the EU-US Data Privacy Framework.

Newsletters are sent only after explicit consent and double opt-in under Article 6(1)(a) GDPR. Consent can be withdrawn through the unsubscribe link or by writing to privacy@passvanta.com. Open and click tracking remains disabled by default. If enabled later, it requires separate transparency and legal assessment. After an unsubscribe, the address may remain on a suppression list to prevent further mail. Consent evidence is generally retained for up to three years after the end of the year in which consent was withdrawn where needed for legal defence.

AI processing with Mistral, OpenAI and Google Gemini

Passvanta may send documents and structured product data to Mistral AI, OpenAI and Google Gemini to extract, classify and summarise content, create quality or plausibility indications and suggest data fields. Provider selection may depend on document type, language, availability and quality. Document content can contain personal data.

For Customer Content, processing takes place on documented instructions and under the Passvanta DPA. For Passvanta's own test or pre-contract processing, the basis is Article 6(1)(b) or (f) GDPR. Special-category data is not intended. Passvanta uses business or API offerings with DPAs and disables voluntary model-training use where an option exists. EEA data processed through OpenAI relies on OpenAI Ireland Limited and safeguards in its DPA. Mistral's commercial DPA applies. Gemini must be used through a suitable Google Cloud contract and Cloud DPA with an EEA-appropriate setup. Consumer AI Studio access without suitable processor terms is not approved for Customer Content.

AI outputs can be inaccurate or incomplete. Passvanta does not make solely automated decisions that produce legal or similarly significant effects for individuals. Users must review outputs before adopting, publishing or relying on them for compliance decisions.

Google Analytics, Google Ads and Meta Pixel

Google Analytics 4, Google Ads conversion tracking and remarketing, and Meta Pixel load only after the visitor has consented to the relevant optional category. Before consent, Passvanta triggers no tags, pixels, SDKs or cookieless pings from these providers. The custom banner therefore uses complete prior blocking, not advanced consent mode transmission without consent.

After consent, the services may process online identifiers, cookie IDs, IP and device information, pages, events, referrers, approximate location, campaign parameters and conversions, and may associate data with existing provider accounts. Depending on the service, the provider is Google Ireland Limited or Meta Platforms Ireland Limited; transfers to affiliated companies in third countries may occur. Storage or access relies on section 25(1) TDDDG and subsequent processing on Article 6(1)(a) GDPR. Consent is voluntary and can be withdrawn at any time through Cookie Settings.

For collecting and transmitting certain event data through Meta Business Tools, Passvanta and Meta Platforms Ireland Limited may be joint controllers under the applicable Meta terms. Passvanta is responsible for lawful collection and transmission on its website; Meta is responsible for its subsequent processing. The essence of the arrangement is described in the Meta Business Tools Terms and Meta Privacy Policy.

Passvanta does not use Meta Conversions API. Google Ads remarketing and Meta Pixel require Marketing consent. Google Analytics requires Analytics consent. Refusal does not restrict necessary features.

Retention

Passvanta retains personal data only for as long as necessary for the relevant purpose. In summary: contract and account data for the contract term and applicable evidence and limitation periods; accounting vouchers generally eight years; business correspondence generally six years; security logs generally 30 days; non-contractual contact requests generally twelve months; Readiness data and uploads without an account generally 30 days; newsletter

data until withdrawal, followed only by necessary suppression and evidence data. Backups are overwritten under the documented cycle and remain restricted until then.

Individual rights and complaint

Individuals have GDPR rights to access, rectification, erasure, restriction, portability and objection. Consent can be withdrawn prospectively at any time. Objections to legitimate-interest processing may be made on grounds relating to the individual's situation. Send requests to privacy@passvanta.com. Passvanta may request additional information where necessary to verify identity securely.

A complaint may be filed with a supervisory authority. The authority generally responsible for Passvanta is Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Heilbronner Straße 35, 70191 Stuttgart, Germany, poststelle@lfdi.bwl.de.

Required data and automated decisions

Contract and account data is required where Passvanta cannot create an account, enter a contract or provide the service securely without it. Other fields are voluntary unless identified as required. Passvanta does not use solely automated decision-making within Article 22 GDPR.

Changes

Passvanta updates this notice when services, providers or law change. Each version carries a date. Material changes are notified in the service or by email where required.

Recipients and international transfers

Recipient	Location	Purpose	Safeguard
Vercel, Inc.	USA; hosting region by account	Web and app hosting	DPA; SCCs or adequacy decision where applicable
Cloudflare, Inc.	USA and global network	DNS, CDN, WAF and security logs	DPA; SCCs or EU-US DPF where applicable
Databricks, Inc. with Neon Platform	USA; database region by project	PostgreSQL database	DPA and SCCs; select an EU region
Plus Five Five, Inc. Resend	USA	All operational and newsletter email	DPA; SCCs and EU-US DPF stated by provider
OpenAI Ireland Limited and affiliates	Ireland and possible third countries	AI extraction and processing	DPA; SCCs or adequacy decision
Mistral AI SAS	France and locations by configuration	AI extraction and processing	DPA; transfer mechanism by configuration
Google Cloud EMEA Limited and affiliates	Ireland and possible third countries	Gemini API	Cloud DPA; SCCs or adequacy decision
IONOS SE	Germany and locations by service	Domain and email-address administration	DPA where IONOS acts as processor

A DPA or SCC clause does not eliminate every third-country risk. Before launch, Passvanta must document relevant transfer impact assessments, any DPF certification used, selected regions and supplementary technical measures.