Privacy Policy

Last Updated: 2026-11-05 Effective Date: 2026-11-05

1. Controller and Contact

1.1. The controller within the meaning of the General Data Protection Regulation (GDPR) is:

Genz IT Solutions GmbH Brückengasse 1b 78462 Konstanz Germany E-mail: mail@genz-its.com

Authorised Managing Director: Robin Marcel Genz

1.2. No Data Protection Officer has been appointed. For data protection inquiries, please contact: legal@hotcodepush.com

2. Scope

2.1. This Privacy Policy applies to the processing of Personal Data of website visitors, prospective customers and account holders by Genz IT Solutions GmbH (**"Provider"**) acting as Controller in connection with HotCodePush, the over-the-air (OTA) update service for React Native, Expo, Capacitor and Cordova (**"Service"**).

2.2. End-user data that the customer's applications transmit to the Service via the HotCodePush SDKs is processed on behalf of the customer. In that regard, the customer is the Controller. The provisions of the Data Processing Agreement (DPA) at https://hotcodepush.com/legal/data-processing-agreement apply. This Privacy Policy does not apply to such data.

2.3. In addition to the GDPR, this Privacy Policy also satisfies the information obligations under the Swiss Federal Act on Data Protection (revFADP). Swiss B2B customers will receive a revFADP addendum to the Data Processing Agreement upon request.

2.4. The Service is directed at businesses and is not intended for children.

3. Processing Activities

3.1. Website Operation and Server Logs

- **Data**: IP address, date and time of access, requested resource, HTTP status code, referrer URL, browser type and version, operating system
- **Purpose**: Provision of the website, the console and the API; ensuring technical security; detection and prevention of misuse
- **Legal basis**: Art. 6(1)(f) GDPR (legitimate interest in the secure provision of the Service)
- **Processing**: Requests are served through the edge network of Cloudflare, Inc. (see Section 5), which records access logs for the Provider.
- **Retention period**: 7 days, then deletion or anonymisation

3.2. Account and Contract Performance

- **Data**: Name, e-mail address, company name, postal address (where provided), login credentials (password hash, second factor where enabled), account settings, organisation and membership data, API tokens; for each sign-in the IP address, user agent and country; the audit log of the organisation (who changed what, when and from which network); the sign-up attribution (Section 4.3)
- **Purpose**: Creation and administration of the customer account, provision of the contractual services, security of the account, communication within the contractual relationship
- **Legal basis**: Art. 6(1)(b) GDPR (performance of contract). For the audit log: Art. 6(1)(f) GDPR (legitimate interest in traceability and security). For the sign-up attribution: Art. 6(1)(f) GDPR (Section 4.3)
- **Retention period**: Duration of the account. A deleted account or organisation is removed from active systems seven days after deletion. Within these seven days support can restore it. Audit log entries are retained for twelve months. Statutory retention obligations remain unaffected (§§ 147 AO, 257 HGB: up to 10 years)

3.3. Payment Processing (Self-Serve) via Merchant of Record

- **Data**: Name, e-mail address, company name, billing address, VAT ID, selected spending cap and usage of the billing month
- **Purpose**: Payment processing, invoicing, tax calculation, refunds
- **Legal basis**: Art. 6(1)(b) GDPR (performance of contract)
- **Recipients**: Polar Software Inc. as Merchant of Record. Polar acts as an independent controller in the purchase process and is not a processor of the Provider. Polar's own privacy policy applies.
- **Retention period**: Stored by the Provider only to the extent necessary for subscription assignment. Payment details (credit card numbers, bank details) are processed exclusively by the Merchant of Record and are not transmitted to the Provider.

3.4. Invoicing and Tax Record Retention (Enterprise)

- **Data**: Name, e-mail address, company name, billing address, VAT ID, invoice line items, payment receipts
- **Purpose**: Direct invoicing, bookkeeping, fulfilment of statutory tax retention obligations
- **Legal basis**: Art. 6(1)© GDPR (legal obligation, §§ 147 AO, 257 HGB)
- **Retention period**: 10 years from the end of the calendar year in which the invoice was issued (§ 147(3) AO)

3.5. Newsletter and Marketing

- **Data**: E-mail address, time of consent, name and company where provided
- **Purpose**: Sending newsletters and product information
- **Legal basis**: Art. 6(1)(a) GDPR (consent) for newsletters. Art. 6(1)(f) GDPR (legitimate interest) in conjunction with § 7(3) UWG (German Unfair Competition Act) for direct marketing to existing customers regarding its own similar services
- **Processing**: Newsletters are sent via Resend (see Section 5). The Provider's own sign-up form records the consent. No third-party sign-up forms are used.
- **Withdrawal**: May be exercised at any time via the unsubscribe link in the newsletter, in the account settings or by e-mail to legal@hotcodepush.com
- **Retention period**: Until withdrawal of consent. After unsubscription the e-mail address is kept on a suppression list, so that it is not written to again and the prior consent can be evidenced, for up to 3 years (legitimate interest, Art. 6(1)(f) GDPR).

3.6. Security and Abuse Prevention

- **Data**: IP addresses, country of the request, access patterns, account activities, security logs
- **Purpose**: Detection and prevention of attacks, misuse and fraud; rate limiting; enforcement of the Acceptable Use Policy; enforcement of the IP and country allowlists a customer has configured for its own organisation
- **Legal basis**: Art. 6(1)(f) GDPR (legitimate interest in the security of the Service). For customer-configured allowlists: Art. 6(1)(b) GDPR (performance of contract)
- **Retention period**: 90 days. In the event of a concrete suspicion, until the conclusion of the investigation

3.7. Support Requests

- **Data**: Name, e-mail address, content of the request, technical information for troubleshooting where applicable, account facts needed to answer the request
- **Purpose**: Handling of support requests, documentation of the support history
- **Legal basis**: Art. 6(1)(b) GDPR (performance of contract) for existing customers. Art. 6(1)(f) GDPR (legitimate interest) for prospective customers
- **Processing**: Requests to support@hotcodepush.com and hello@hotcodepush.com are classified and a first reply is drafted by the Provider's AI assistant "Hanna". An engineer of the Provider approves every reply before it is sent, and the sender can reach a person at any time by writing "human". The drafting runs on models hosted by Scaleway SAS on its Generative APIs in Paris, France. Draft replies are approved in the Provider's Slack workspace (see Section 5). Questions asked publicly in GitHub Discussions or in the issue trackers of the SDK repositories are public, together with the asker's GitHub profile.
- **Retention period**: Raw e-mails of a support case are deleted 90 days after the case is closed. The redacted question and the reply sent are retained for the duration of the contractual relationship plus 3 years (standard limitation period, § 195 BGB). The mailbox retains the correspondence for the same period.

3.8. Product Analytics and Telemetry

- **Data**:
  - *Product analytics (console)*: usage events (features used, actions performed, pages viewed) linked to the account holder's user ID and organisation ID, together with the sign-up attribution without the advertising click identifiers (Section 4.3)
  - *CLI telemetry*: anonymous usage data (command invoked, outcome, duration, CLI version, whether the command ran in a CI environment, framework used) and crash reports (error code and stack trace, with paths and arguments stripped, see Section 3.9)
- **Purpose**: Understanding feature usage, product improvement, error detection, capacity planning
- **Legal basis**: Art. 6(1)(f) GDPR (legitimate interest in improving and securing the Service)
- **Processing**: Product analytics events are recorded server-side and processed by PostHog on its EU infrastructure (see Section 5). No analytics cookies or other identifiers are stored on the user's device for this purpose. Identifiers of end-user devices of the customer's applications are never sent to the analytics provider. Where AI-assisted analytics features are used, PostHog may process this data via AI sub-processors. This data is not used to train third-party AI models (see Section 5).
- **Opt-out**: Account holders may object to product analytics at any time (Art. 21 GDPR). CLI telemetry is switched off by setting the environment variable `HOTCODEPUSH_TELEMETRY_DISABLED=1` or `DO_NOT_TRACK=1`.
- **Retention period**: Product analytics: for the duration of the account. When an account is deleted, the Provider deletes the associated analytics profile including its events at the analytics provider. CLI telemetry is anonymous and carries no identifier that links it to a person.

3.9. Error Monitoring

- **Data**: Error messages, stack traces, affected request path, browser or runtime version. Cookies, request bodies, user data and the IP address are not transmitted. Headers and query parameters are filtered against a personal-data deny list before sending.
- **Purpose**: Detection and correction of errors in the Service
- **Legal basis**: Art. 6(1)(f) GDPR (legitimate interest in a stable Service)
- **Recipients**: Sentry (see Section 5)
- **Retention period**: 90 days

3.10. Status Page

- **Data**: When visiting status.hotcodepush.com, the status page provider processes the visitor's IP address and technical browser data under its own privacy policy. Subscribers to status notifications provide their e-mail address to the provider.
- **Purpose**: Public information on the availability of the Service
- **Legal basis**: Art. 6(1)(f) GDPR (legitimate interest in transparent availability information)
- **Recipients**: UptimeRobot (see Section 5)
- **Retention period**: Governed by the status page provider's own terms

3.11. Sign-in via Third-Party Identity Providers

- **Data**: Profile data transmitted by the identity provider (typically name, e-mail address, profile picture, user ID)
- **Purpose**: Authentication and account creation or linking
- **Legal basis**: Art. 6(1)(b) GDPR (performance of contract)
- **Recipients**: The respective identity provider receives the information that the user is signing in to the Service. The Provider offers sign-in via the following providers:
  - GitHub — Privacy Policy
  - Google — Privacy Policy
  - An organisation's own OpenID Connect or SAML identity provider, configured by the customer. That provider is engaged by the customer and is not a recipient of the Provider.
- **Retention period**: The transmitted profile data is stored for the duration of the account. Deletion at the identity provider is governed by that provider's own terms.

4. Device Access (§ 25 TDDDG)

4.1. **Website without cookies**: The Provider's public website sets no cookies. Reach measurement uses PostHog in cookieless mode: no identifiers are stored on the visitor's device for this purpose. Visits are counted using a daily-changing, non-reversible hash value generated on PostHog's servers, and the visitor identity is held in page memory only. The analytics script transmits the page visited, the referrer and technical characteristics of the browser and device (e.g. screen resolution, time zone, language). The data is used solely for the aggregated measurement of the Provider's own website. No cross-site profiles are created. Legal basis: § 25(2) no. 2 TDDDG (German Telecommunications Digital Services Data Protection Act). For the subsequent processing: Art. 6(1)(f) GDPR (legitimate interest in reach measurement). See Section 5 for details on PostHog.

4.2. **Console**: The console uses browser-side storage exclusively for strictly necessary functions:

- **Session cookie**: The API sets one HttpOnly session cookie that keeps the user signed in. Legal basis: § 25(2) no. 2 TDDDG (strictly necessary for the service explicitly requested by the user). Duration: until logout or expiry of the session.
- **User preferences** (localStorage): Storage of interface preferences (e.g. theme, language). Legal basis: § 25(2) no. 2 TDDDG. Duration: Until manual deletion by the user.

4.3. **Advertising attribution**: The website, including the documentation, records where a visit came from, so that a later sign-up can be attributed to the advertisement or channel that led to it. No cookie is set, and no advertising script runs on the website. Legal basis for the processing: Art. 6(1)(f) GDPR (legitimate interest in measuring which advertisements and channels lead to sign-ups).

- **Record in the browser** (`localStorage`): on the first visit the referring website (domain only), the first page visited (path only), the UTM source and campaign carried in the URL and, where an advertisement led to the visit, the click identifier of Google, Reddit, Meta or X. A later visit from an advertisement adds or replaces the click identifier of that platform, so the record holds at most the most recent one per platform. The rest of the record stays unchanged. Legal basis for the storage: § 25(2) no. 2 TDDDG. Duration: until the visitor clears the browser's site data.
- **Sign-up**: A link from the website to the console carries the record. At sign-up it is stored on the account for the duration of the account (Section 3.2). The referring website, the first page, the source and the campaign are added to the account holder's analytics profile (Section 3.8). The click identifiers are not. They remain on the account so that a later purchase can be attributed to the same advertisement. A report of purchases to the advertising platforms would be described in this Privacy Policy first.
- **Conversion report**: A few hours after sign-up, if the account's e-mail address is verified by then, the Provider reports each click identifier server-side as a sign-up to the advertising platform it belongs to: Google (Google Ads), Reddit (Reddit Ads), Meta (Meta Ads) or X (X Ads) (see Section 5). The report contains the click identifier, the time of the sign-up and a pseudonymous identifier of the account. The report to Meta also contains the user agent of the browser used for the sign-up (see Section 3.2), which Meta's Conversions API requires. No name, e-mail address or IP address is transmitted. For the transmission of the report to Meta, the Provider and Meta Platforms Ireland Limited are joint controllers under Art. 26 GDPR. The essence of that arrangement is set out in Meta's Controller Addendum at https://www.facebook.com/legal/controller_addendum. After receipt, Meta processes the data as an independent controller. Data subjects may exercise their rights against either party.

5. Recipients and Third-Party Services

5.1. The Provider uses the following recipients for the provision of its own services. The list below relates exclusively to data that the Provider processes as Controller. The sub-processor list for customer data processed by the Provider on behalf of customers is available at https://hotcodepush.com/legal/subprocessors.

Recipient	Purpose	Location	Transfer mechanism
Cloudflare, Inc.	Website and API delivery, CDN, DDoS protection, DNS, e-mail routing	USA (data stored in the EU)	EU-US Data Privacy Framework (DPF-certified)
PlanetScale, Inc.	Database services (data stored in Frankfurt, Germany)	USA	EU-US Data Privacy Framework (DPF-certified)

Scaleway SAS	Cloud infrastructure (compute, storage), backups, mailboxes, AI models for support mail processing (Generative APIs)	France, EU	Adequacy (EU)
Hetzner Online GmbH	Cloud infrastructure (compute, storage), backups	Germany, EU	Adequacy (EU)
Resend (Plus Five Five, Inc.)	E-mail delivery (transactional and newsletter)	USA	EU-US Data Privacy Framework (DPF-certified)
PostHog (PostHog, Inc.)	Product and web analytics	Germany, EU (operator: PostHog, Inc., USA)	EU-US Data Privacy Framework (DPF-certified)
Sentry (Functional Software, Inc.)	Error monitoring	USA	EU-US Data Privacy Framework (DPF-certified)
UptimeRobot s. r. o.	Status page and availability monitoring	Slovakia, EU	Adequacy (EU)
GitHub, Inc.	Sign-in, public discussions and issue trackers	USA	EU-US Data Privacy Framework (DPF-certified)
Google LLC	Sign-in, conversion measurement for advertisements (Google Ads)	USA	EU-US Data Privacy Framework (DPF-certified)
Reddit, Inc.	Conversion measurement for advertisements (Reddit Ads)	USA	EU-US Data Privacy Framework (DPF-certified)
Meta Platforms Ireland Limited, Meta Platforms, Inc.	Conversion measurement for advertisements (Meta Ads), joint controllership (Section 4.3)	Ireland, EU and USA	EU-US Data Privacy Framework (DPF-certified)
X Corp.	Conversion measurement for advertisements (X Ads)	USA	EU-US Data Privacy Framework (DPF-certified)
Slack Technologies, LLC	Internal approval of support replies	USA	EU-US Data Privacy Framework (DPF-certified)

5.2. For all US recipients with DPF certification, the EU-US Data Privacy Framework serves as the primary transfer mechanism. Where a recipient's terms also include EU Standard Contractual Clauses (SCCs) 2021/914, they apply as a fallback.

5.3. **Identity providers**: GitHub and Google are listed as recipients in the sign-in flow in Section 3.11.

5.4. **Merchant of Record**: Polar Software Inc. acts as an independent controller in the purchase process, not as a processor of the Provider. Its privacy policy is available on its website.

5.5. **PostHog AI sub-processors**: Where AI-assisted analytics features are enabled, PostHog may process analytics data using AI sub-processors located in the USA. These providers do not use the data to train their models. Transfers are safeguarded by EU Standard Contractual Clauses under PostHog's data processing agreement. Certain providers are additionally certified under the EU-US Data Privacy Framework. The current list of PostHog's sub-processors is available at https://posthog.com/subprocessors.

6. International Data Transfers

6.1. Where Personal Data is transferred to recipients outside the EEA, the Provider ensures that an adequate level of data protection is maintained.

6.2. For US recipients certified under the EU-US Data Privacy Framework, an adequacy decision of the European Commission applies (Implementing Decision (EU) 2023/1795 of 10 July 2023).

6.3. Where no adequacy decision exists, EU Standard Contractual Clauses (Implementing Decision (EU) 2021/914) are used as the transfer mechanism.

6.4. **Switzerland**: For transfers from Switzerland, the Provider relies on the Federal Council's adequacy decision on the EU-US Data Privacy Framework (in force since 15 September 2024) or on the Standard Contractual Clauses with Switzerland-specific amendments.

7. Data Subject Rights

7.1. Data Subjects have the following rights under the GDPR:

- **Access** (Art. 15 GDPR): Right to confirmation and information about the data processed
- **Rectification** (Art. 16 GDPR): Right to correction of inaccurate data
- **Erasure** (Art. 17 GDPR): Right to erasure, provided no statutory retention obligation prevails
- **Restriction** (Art. 18 GDPR): Right to restriction of Processing
- **Data portability** (Art. 20 GDPR): Right to receive one's own data in a machine-readable format
- **Objection** (Art. 21 GDPR): Right to object to Processing based on legitimate interests

7.2. Consent given may be withdrawn at any time with effect for the future, without affecting the lawfulness of the Processing carried out prior to the withdrawal.

7.3. **Right to lodge a complaint**: Data Subjects have the right to lodge a complaint with a Supervisory Authority. The competent Supervisory Authority for the Provider is:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) Lautenschlagerstraße 20 70173 Stuttgart https://www.baden-wuerttemberg.datenschutz.de

For Data Subjects in Switzerland, the Swiss Federal Data Protection and Information Commissioner (FDPIC) is the competent authority.

8. No Automated Decision-Making

8.1. The Provider does not employ automated decision-making including profiling within the meaning of Art. 22 GDPR that produces legal effects concerning Data Subjects or similarly significantly affects them. The AI-assisted drafting of support replies under Section 3.7 is reviewed by a person before any reply is sent.

9. Contact for Data Protection Inquiries

9.1. For all data protection inquiries, please contact:

Genz IT Solutions GmbH legal@hotcodepush.com

10. Amendments to this Privacy Policy

10.1. The Provider reserves the right to amend this Privacy Policy where required by changes in processing activities, legal requirements or technical developments. The current version is available at https://hotcodepush.com/legal/privacy-policy.

10.2. In the event of a sale, merger or transfer of a business unit, the Provider may transfer Personal Data to the acquirer or successor where necessary to continue the contractual services. The existing data protection standards shall remain in effect. In such a case, the Provider shall inform Data Subjects in advance.