Security Policy

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

1. Hosting and Encryption

1.1. The production infrastructure of HotCodePush is operated with carefully selected infrastructure providers. The current list is set out in Annex 3 to the Data Processing Agreement. Bundles and the data the Provider stores are held in the European Union. Requests from end-user devices are served from the edge location nearest the device.

1.2. All data in transit is encrypted using TLS 1.2 or higher.

1.3. Data at rest is encrypted using industry-standard methods (encryption at rest).

2. Access Control

2.1. All administrative access to production systems requires multi-factor authentication (MFA).

2.2. Access rights are granted on a least-privilege basis and reviewed on a regular basis.

3. Handling of Customer Data

3.1. **Bundles**: Bundles are stored solely to deliver updates to the customer's apps and are processed for no other purpose. The Provider's personnel (including contractors) shall only access the contents of a bundle in a support case with the express consent of the customer.

3.2. **Code signing**: The Provider supports code signing of bundles. Customers may sign their bundles with their own RSA key pair. Where enabled by the customer, the SDK verifies the signature on the device before applying the update. The private key remains with the customer and is never transmitted to the Provider.

3.3. **Fail-Open**: An installed app never depends on the availability of HotCodePush. An outage, a reached spending cap, or a suspended account stops the delivery of new updates only. Devices keep running the update they have.

3.4. **No AI/ML training**: The Provider does not use customer data (including bundles and the data the SDK reports from end-user devices) for training, fine-tuning, or improving AI or ML models.

4. Certifications and External Audits

4.1. The Provider undergoes annual **SOC 2 Type II** audits and holds **ISO 27001** certification. Both cover HotCodePush. The compliance documentation is available at https://trust.genz-its.com. The current SOC 2 report is available on request under NDA.

4.2. From 2026 onwards, **annual external penetration tests** are conducted. Reports are available on request under NDA.

5. Incident Response

5.1. The Provider maintains a documented incident response process covering detection, containment, remediation, and post-incident review.

5.2. In the event of a security incident affecting customer data, the customer shall be notified without undue delay. For personal data breaches, the notification obligations set out in DPA §10.1 apply (48-hour deadline).

5.3. In the event of a security incident affecting confidential customer materials (in particular unreleased bundles or API tokens), a separate notification shall be provided in accordance with the confidentiality provisions of the Terms of Service (Section 9), regardless of whether personal data is affected.

6. Vulnerability Disclosure

6.1. The Provider welcomes the responsible disclosure of security vulnerabilities. Reports shall be sent to: security@hotcodepush.com. The contact is also published at https://hotcodepush.com/.well-known/security.txt.

6.2. **Testing boundaries**: Security researchers shall observe the following boundaries:

- no denial-of-service attacks against production systems,
- no access to other customers' data,
- no exploitation beyond proof of concept.

6.3. **Safe harbour**: The Provider shall not pursue civil claims and shall not file a criminal complaint against security researchers who act in good faith within the boundaries set out above.

7. Contact

7.1. Security incidents and vulnerability reports: security@hotcodepush.com

7.2. This document serves transparency and trust-building purposes. It is not contractually binding. The binding technical and organisational measures are set out in the Data Processing Agreement (Annex 2).