Acceptable Use Policy

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

1. Scope

1.1. This Acceptable Use Policy (**"AUP"**) applies to the use of HotCodePush, the over-the-air (OTA) update service provided by Genz IT Solutions GmbH (**"Provider"**).

1.2. This AUP supplements the General Terms and Conditions (GTC). In the event of a conflict, the GTC shall prevail.

2. Prohibited Content

2.1. The Customer shall not distribute, store, or process any content through HotCodePush that:

- contains or distributes malware, viruses, trojans, spyware, ransomware, or phishing components,
- violates applicable law, in particular criminal law, youth protection law, or export control regulations,
- is discriminatory, defamatory, harassing, or glorifies violence,
- infringes copyrights, trademarks, patents, or personality rights of third parties.

3. Prohibited Activities

3.1. The following activities are prohibited when using HotCodePush:

- **Circumvention of app store guidelines**: Using HotCodePush to circumvent review or approval processes of Apple or Google. An OTA update must not change the primary purpose of the app. The Customer shall in particular comply with the Apple App Store Review Guideline 2.5.2 and the Google Play "Device and Network Abuse" Policy.
- **Reverse engineering**: Decompilation, disassembly, or other reverse engineering of the HotCodePush service beyond the extent mandated by applicable law. The open-source SDKs and tools are governed by their respective open-source licences.
- **Unauthorised load and penetration testing**: Conducting load or security tests against the HotCodePush infrastructure without prior written approval from the Provider.
- **Resource abuse**: Using the HotCodePush infrastructure for purposes that do not correspond to its intended use, in particular crypto-mining, covert data processing in bundles, use of the update infrastructure as general file hosting, or other resource-intensive third-party use.
- **Circumvention of billing limits**: Circumventing the spending cap, the MAU ceiling of the Free plan, or the fair-use thresholds under Section 2.2 of the GTC, in particular by splitting one app across several organisations or accounts to multiply free MAU, by manipulating the device identifiers reported by the SDK, by account sharing to circumvent limits, or by automated scraping of the platform.
- **Spam**: Sending unsolicited messages or mass communications through HotCodePush.
- **Attacks on third parties**: Using HotCodePush to conduct attacks against third parties or their infrastructure.

4. Customer Obligations

4.1. The Customer shall ensure that its use of HotCodePush complies with all applicable laws and regulations, including the applicable app store guidelines of Apple and Google.

4.2. The Customer is responsible for securing its account and access credentials. The Customer shall notify the Provider without undue delay of any unauthorised use that comes to its attention.

5. Reporting Abuse and Takedown

5.1. Violations of this AUP and notices of illegal content may be reported to legal@hotcodepush.com. The Provider shall review incoming reports and, where there is reasonable suspicion, initiate the measures described in Section 6.

5.2. Bundles hosted through HotCodePush are content that the Provider distributes to end-user devices on the Customer's behalf. Upon a substantiated notice that a bundle contains illegal content or infringes third-party rights (including notices of

copyright infringement), the Provider may stop distribution of the affected bundle. Apps that already run the bundle keep running it. The Provider does not modify or remove content on end-user devices (Section 6.3). The Provider shall inform the Customer without undue delay of the notice and the measure taken. The Customer may respond. The Provider shall review the response and restore distribution if the notice proves to be unfounded.

6. Enforcement

6.1. In the event of violations of this AUP, the Provider shall take graduated measures:

- Warning and request to cease the violation,
- Blocking of individual affected content or features,
- Temporary suspension of the account,
- Termination for cause of the contractual relationship.

6.2. In the event of an acute threat (in particular ongoing distribution of malware, active attacks on third parties, or imminent legal violations), the Provider shall be entitled to take immediate measures without prior warning. The Customer shall be notified without undue delay of the measure taken and the reason for it.

6.3. A suspension of the account or a block of content stops the delivery of new updates and the use of the console, the API, and the CLI. Apps already installed keep running the update they have. No measure under this AUP breaks installed apps.

7. Amendments to this AUP

7.1. The Provider may amend this AUP. The amendment procedure, right of objection, and legal consequences set out in the GTC (Section 17) shall apply accordingly.

7.2. In the event of material restrictions under this AUP, the Customer shall have the right to terminate for cause with effect from the date on which the amendment takes effect.

7.3. The authoritative language version of this Acceptable Use Policy is the English version. The German version is for informational purposes only.