

STABILO Highlight App

Date: 2026-10-19 | Version: 1.3

1. Product with digital elements

Product / service	STABILO Highlight App (iOS/Android) with the associated cloud services (backend, AI processing, STABILO Account)
Manufacturer / provider	STABILO International GmbH, Schwanweg 1, 90562 Heroldsberg, Germany
Contact (general)	Data protection: datenschutz@schwan-stabilo.com / Reports and requests: form at https://www.stabilo.com/com/data-act-cra/#nav-formular

2. Support period and security updates

- **Support period:** Security updates at least until 12/2032. As long as the product is being sold, we review this date annually and extend it where appropriate; an end date that has already been stated will not be shortened. Applies to the current app version and the associated cloud services.
- **Type of security support:** security updates for the app via new app versions; security updates and configuration changes to the backend (hosted in Europe) and to the integrated services for text recognition and generative AI.
- **Update mechanism:** App updates via the Apple App Store or Google Play – automatic if automatic updates are enabled in the device/store settings (where they can also be disabled). Server-side updates are applied centrally without any action by users.
- **Note:** Each security update remains available for at least 10 years after its release or for the remainder of the support period, whichever is longer.

3. Single point of contact for vulnerabilities

Vulnerability contact	Form at https://www.stabilo.com/com/data-act-cra/#nav-formular
CVD policy URL	https://www.stabilo.com/com/data-act-cra/
Optional: PGP key	Not currently offered

4. Coordinated vulnerability disclosure (CVD) – brief process

- **How to report:** via the form at <https://www.stabilo.com/com/data-act-cra/#nav-formular>; please state the product and version. No user account is required; an email address is only needed for follow-up questions and feedback. Please do not report vulnerabilities via general support channels, social media or app store reviews.
- **What to include:** app version, device and operating system version, description of the vulnerability, possible impact, proof of concept or steps to reproduce (if possible), log excerpts without unnecessary personal data.

- **Feedback:** If an email address was provided: acknowledgement of receipt within 2 working days, initial assessment within 10 working days, followed by regular status updates until the issue is resolved.
- **Responsible disclosure:** We ask you to coordinate the timing of any publication with STABILO. The full rules, including our commitment to reporters, are available at <https://www.stabilo.com/com/data-act-cra/>. Please test only with your own accounts and devices, do not access other users' data and do not disrupt operations.
- **Reporting obligations:** STABILO reports actively exploited vulnerabilities and severe security incidents to the competent CSIRT and to ENISA in accordance with Art. 14 CRA and informs affected users.

5. Information and secure use

- **Secure installation and operation:** Install the app only from the Apple App Store or Google Play; Android and iOS are supported. The camera permission is needed for scanning. Sign-in with the STABILO Account takes place in the device's system browser, not within the app; use a unique, secure password and keep the operating system up to date.
- **Configuration:** Keep automatic app updates enabled (recommended). Share links only selectively, as anyone with the link can see the shared content. Permissions can be revoked in the system settings.
- **Logging/diagnostics:** The app uses Firebase, including Crashlytics for crash reports. Server logs are stored for a maximum of 3 days unless they are needed for security or to investigate an incident. For support we need the app version, device and operating system version, the email address of the STABILO Account, and the time and description of the error – no passwords or sensitive scan content.
- **Intended use:** photographing printed texts that have been marked with STABILO highlighters; the highlighter colour determines the AI function (summarise, explain, translate, quote). Not intended for text on screens. The AI functions require an internet connection. An AI model detects the highlighter colour and the marked areas; text recognition is performed via Google Vision OCR, the generative functions via Google Gemini. Photographed content is not used to train the recognition model; use by Google for training purposes is excluded as far as contractually and technically possible.
- **Foreseeable risks:** Please do not photograph or capture health data, access credentials or passwords.
- **Secure decommissioning:** Content (images, texts, highlights) can be deleted in the app at any time. The STABILO Account can be deleted directly in the account management at any time; alternatively, deletion can be requested via the form at <https://www.stabilo.com/com/data-act-cra/#nav-formular> or at datenschutz@schwan-stabilo.com. After the account has been deleted, the content is deleted within 30 days. Then uninstall the app. Accounts without login or use are considered inactive after 3 years and are deleted following a notification 30 days in advance.

6. EU declaration of conformity

- **EU Declaration of Conformity:** in future at <https://www.stabilo.com/com/declaration-of-conformity/>.

- **CE marking:** Will be added with the EU declaration of conformity under the CRA, at the latest for versions placed on the market from 11 December 2027.

7. Publication

- **Product page / checkout:** <https://www.stabilo.com/com/products/highlights/stabilo-highlight-app/> – section “Cybersecurity & Support” including the support period
- **In-app:** Settings → “Security & Support” with vulnerability contact, link to the CVD policy and support period (in preparation).
- **Support page:** “Security, Support and Data Access” page at <https://www.stabilo.com/com/data-act-cra/> with one section per product; this document is versioned (date/version in the header).