

Privacy Policy

Bluecode Software

Version April 2025

(SDK VAS)

Data Controller

The entity responsible for the collection and processing of personal data in connection with the Bluecode Software is:

Blue Code International AG
Commercial Registry Office Schwyz; CHE-281.323.867
Schützenstrasse 7, 8853 Lachen, Switzerland

Data protection representatives in the EU within the meaning of Art. 27 GDPR as a point of contact for supervisory authorities and data subjects for all questions in connection with EU data protection law:

Secure Payment Technologies GmbH
FN 364923 b, Commercial Court Innsbruck
Müllerstraße 27, 6020 Innsbruck, Austria
E-mail: datenschutz@spt-payments.com

Data Collection When Using the Bluecode Software in an App

The term "Bluecode Software" refers to the software module that enables Bluecode payment functionality, including optional value-added services (e.g., integration with loyalty programs), embedded in a mobile app. In this document, any app using the Bluecode Software is referred to as a "Bluecode-enabled app".

We, Blue Code International AG, are committed to respecting the privacy of all individuals using Bluecode payment features in Bluecode-enabled app.

We only process technical data as described in the "Data Collection" section below. We do not know your identity (i.e., your name as a Bluecode user).

If you use "Minis" (third-party value-added services), personal data may be required by the third-party provider. In such cases, only the provider's privacy policy applies. Blue Code International AG does not process this data.

To ensure safe and full use of the Bluecode payment feature within an Bluecode-enabled app, processing certain technical data is necessary (see "Data Collection"). The extent of this data processing also depends on which features you use and the consents you have given (e.g., location data).

We strictly comply with all applicable data protection and security regulations, including the relevant EU laws. All personal information is treated confidentially and in accordance with legal requirements.

The Privacy Policy and Terms of Use for the Bluecode payment function and SEPA direct debit mandate are provided during the registration process and are agreed upon with the respective issuer, not with us.

Data collection

When you use the Bluecode Software in a Bluecode-enabled app, we collect the following technical data to provide the mobile payment services and ensure stability and security (legal basis: performance of a contract under Art. 6(1)(b) GDPR):

- IP address
- User agent (browser and operating system)
- Location data (based on GPS or IP address)
- Unique advertising identifiers for iOS and Android devices (IDFA/Android Advertising ID)
- Date and time of requests
- Content of the request (specific page view or activity)
- Access Status/HTTP Status Code
- amount of data transferred in each case
- Language (so-called locale)
- Operating system and version

IP addresses are necessary to establish communication between your device and our servers. They are stored only for the duration of the session.

Location data enables us to show nearby merchants that accept Bluecode and provide localized offers. Transmission is encrypted. The legal basis is the performance of the contract in order to be able to offer an unrestricted use of the Bluecode Software in accordance with Art. 6 (1) (b) GDPR as well as our legitimate interest in optimizing the software or providing advertising that is of interest to you (Art. 6 (1) (f) GDPR).

The unique advertising identifiers for iOS (Identifier for Advertiser (IDFA) and Android Advertising ID (AAID) devices are random device identifiers that the operating system assigns to a user's device. These are used to track the user's use of the Bluecode-enabled app and to recognize them without revealing any personal information. The information is used to provide you with personalized advertisements. The legal basis is our legitimate interest in providing advertising that is of interest to you in accordance with Art. 6 (1) (f) GDPR.

We collect usage statistics (e.g., session duration, app interactions) to improve features and tailor advertising. The legal basis is our legitimate interest in optimizing our software functions in accordance with Art. 6 (1) (f) GDPR.

Permissions

To enable full functionality, the following device permissions may be required:

- **Advertising IDs:** for personalized ads (see "Analytics Tools – Retargeting")
- **Location:** to show relevant merchants and offers
- **Internet:** to be able to offer all functions within the Bluecode Software
- **Camera:** to scan QR codes
- **Network status:** to check online availability

Data is processed based on your consent (Art. 6(1)(a) GDPR) or for contract fulfillment (Art. 6(1)(b) GDPR), as well as our legitimate interests (Art. 6(1)(f) GDPR).

Changes to This Privacy Policy

We reserve the right to update this policy due to legal changes, new technologies, or tool usage. The current version is always available in the Bluecode-enabled app under Settings → Privacy.

Data Recipients and International Transfers

Your data may be shared only with contracted processors based on valid agreements (Art. 6(1)(b)) as well as our legitimate interest in optimizing the Software Art. 6(1)(f) GDPR. Generally, your data is not transferred outside the EEA.

When using the following applications, data may be transferred to third countries:

- Sentry.io (fault tracking and alerting)
- Mixpanel (data evaluation and visualization)

The specific details on data transfer can be found in this privacy policy at the respective points of the individual functions ("Use of analysis tools").

In order to comply with legal obligations, information may be passed on to appropriate government agencies, e.g. in criminal proceedings by judicial order (the legal basis is the fulfilment of a legal obligation pursuant to Art. 6 para. 1 lit. c GDPR).

Use of Analytics Tools

We use third-party providers that may process your data in the United States. The European Commission has deemed companies certified under the EU-U.S. Data Privacy Framework as having an adequate level of data protection. A list of certified companies is available at: <https://www.dataprivacyframework.gov/s/participant-search>

Sentry.io

We use the error tracking tool Sentry, provided by Functional Software Inc., 45 Fremont Street, 8th Floor, San Francisco, California 94105, USA. Sentry enables real-time monitoring of technical issues in web and mobile apps. It allows developers to detect, reproduce, and fix crashes, thereby helping to improve Bluecode-enabled app stability by identifying system errors and monitoring performance.

Sentry is used exclusively for these technical purposes and not for advertising or marketing.

When a malfunction or irregularity is detected, we may temporarily record your interactions with our online services in order to identify and resolve the issue. This process may involve the collection of usage data, IP addresses, and device identifiers. However, such data is immediately anonymized, used only in a non-personal context, and is automatically deleted after 90 days.

The legal basis for this processing is our legitimate interest in ensuring a stable and user-friendly app experience, as outlined in Art. 6(1)(f) GDPR.

For more information, please refer to Sentry's Privacy Policy and Data Processing Addendum: <https://sentry.io/privacy/> and <https://sentry.io/legal/dpa/>.

Mixpanel

We use Mixpanel, a data analytics platform provided by Mixpanel, Inc., Pier 1, Bay 2, The Embarcadero, San Francisco, California 94111, USA. Mixpanel helps us analyze app usage patterns and visualize data, enabling us to optimize and continuously enhance the app's user experience.

All data processed by Mixpanel is pseudonymized—no personally identifiable information (such as names) is collected, and IP addresses are shortened before processing. The data is associated only with a pseudonymized technical identifier. Any identifiers sent to Mixpanel are encrypted using hashing techniques and stored as non-identifiable character sequences. These identifiers are not used to identify individual users and are not linked with any other personal data.

Data collected via Mixpanel is not shared with third parties, and both storage and processing occur in the United States.

The use of Mixpanel is carried out to optimize the user-friendliness of the software and thus represents a legitimate interest within the meaning of Art. 6 (1) (f) GDPR.

For more details, see Mixpanel Inc.'s Privacy Policy and Data Processing Addendum: <https://mixpanel.com/legal/privacy-policy/> and <https://mixpanel.com/legal/dpa/>.

Retargeting

We use retargeting technology to show users of the Bluecode-enabled app personalized ads and offers when they visit other websites, such as search engines or social media platforms.

Each mobile device has a unique advertising identifier (IDFA for iOS or AAID for Android). This ID can be read by apps and passed to advertising networks. When Bluecode shares this ID with an advertising provider (e.g., Google), and that provider detects the same ID from another app or browser, it recognizes that you have previously used Bluecode. This allows it to show you personalized ads, such as retargeting banners.

Your explicit consent is required before we can use these advertising identifiers. We use this feature to provide relevant advertising based on your interests.

You can disable or limit the use of advertising IDs at any time:

iOS: Go to Settings > Privacy > Tracking, and deactivate "Allow apps to request to track."

Android: Go to Settings > Privacy > Ads, and select "Disable personalized ads" or "Reset advertising ID."

Please note that disabling IDFA or AAID may limit certain functionalities within the Bluecode Software.

The legal basis is your consent to the use of advertising IDs in accordance with Art. 6 (1) (a) GDPR as well as our legitimate interest in being able to display advertising that is of interest to you in accordance with Art. 6 (1) (f) GDPR).

Data Retention and Deletion

We store data only as long as necessary to fulfill the intended purpose (full use of the Bluecode Software). Where statutory retention periods apply (e.g., for tax or corporate law), data is stored for the legally required duration (Art. 6(1)(c) GDPR).

Data Security

We implement technical and organizational measures to protect your data against loss, destruction, manipulation, and unauthorized access. All employees and third parties involved in data processing are bound to confidentiality and legal compliance. When personal data is transmitted, it is encrypted to prevent misuse.

Your rights

As a data subject, you are entitled to the following rights:

- Right of access (Art. 15 GDPR): Inquire whether and to what extent we process your personal data.
- Right to rectification (Art. 16 GDPR): Request correction of inaccurate data.
- Right to erasure (Art. 17 GDPR): Request deletion of your personal data.
- Right to restriction (Art. 18 GDPR): Request restricted processing of your data.
- Right to data portability (Art. 20 GDPR): Receive your data in a structured, machine-readable format and transfer it to another controller.
- Right to withdraw consent (Art. 7(3) GDPR): Withdraw consent at any time without affecting prior lawful processing.
- Right to object (Art. 21 GDPR): Object to data processing based on public interest or legitimate interest grounds.

To exercise your rights or for questions regarding data processing, contact:

Email: datenschutz@spt-payments.com

We will respond without delay, and at the latest within one month. This deadline may be extended by two months in complex cases. You will be informed of any delay and the reasons. You may also lodge a complaint with your national data protection authority.

You also have the right to file a complaint with your national data protection authority.