

# **Privacy Policy**

## **Bluecode App**

**Version April 2025**

We appreciate your interest in Bluecode and want to make sure that you feel safe using the Bluecode App. We take the protection of your personal data very seriously. Compliance with applicable data protection regulations (GDPR, BDSG, DSG) is a fundamental obligation for us.

In the following, we would like to explain in detail how your personal data is collected and processed in the Bluecode App.

### **Data Controller**

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

Secure Payment Technologies GmbH  
Company registration No.: FN 364923 b, Commercial Court Innsbruck  
Müllerstraße 27, 6020 Innsbruck, Austria  
E-mail: [datenschutz@spt-payments.com](mailto:datenschutz@spt-payments.com)

## **Data collection in the Bluecode App**

### **Data Collection When Downloading the Bluecode App**

When you download the Bluecode App, standard information is transmitted to the respective app store (e.g., Apple App Store, Google Play Store), including your username, email address, customer account number, time of download, and your device's unique identifier. We have no control over this data collection and are not responsible for it.

### **Data Collection During App Usage**

Personal data includes any information relating to an identified or identifiable natural person (known as a "data subject").

In order to enable a connection between your device and our servers, we collect your IP address and the unique advertising identification number for iOS and Android devices (IDFA/Android Advertising ID).

To enable a connection between your device and our servers, we collect your IP address and the advertising ID specific to iOS or Android devices (IDFA/Android Advertising ID). The IP address is an online identifier assigned by your internet provider and allows your device to be uniquely addressed online. It is stored for the duration of your session to ensure full App functionality (legal basis: performance of a contract under Art. 6(1)(b) GDPR).

We use push notifications to inform you of relevant actions within the App and provide additional information that may be of interest. Your consent is required for this purpose. On Android devices, push notifications are enabled by default but can be disabled during registration or later

via the app's profile settings. On Apple devices, permission is requested by default and activated based on your choice (legal basis: consent under Art. 6(1)(a) 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>

### **Adjust (up to App Version 6.4)**

We use the analytics service adjust.io by Adjust GmbH to analyze app usage and optimize advertising campaigns. Data includes App downloads, source of download, app open times, usage duration, and frequently used features. Adjust uses anonymized IDFA/Android ID and hashed IP/MAC addresses. Data is stored on Adjust servers in Germany and deleted after 14 days. The legal basis is Article 6(1)(f) GDPR, as we have a legitimate interest in gaining a deeper understanding of how the App functions and is used, better understanding of our users, and delivering an App experience that is more closely aligned with your needs and preferences.

More info: <https://www.adjust.com/privacy-policy/>

Opt-out: <https://www.adjust.com/forget-device/>

### **Microsoft Visual Studio App Center**

We use Visual Studio App Center Diagnostics & Analytics, a service by Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA, to ensure error-free app operation.

Crash reports include technical data such as the error's location in the source code, user actions prior to the crash, app version, and device model. These do not contain personal data or logs and cannot be traced to specific users. Data is deleted after 90 days. (Legal basis: legitimate interest under Art. 6(1)(f) GDPR)

More information:

<https://privacy.microsoft.com/de-de/privacystatement>

<https://learn.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses#microsoft-and-european-union-model-clauses>

### **Google Analytics for Firebase**

We use Google Analytics for Firebase by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, to monitor user behavior and App performance. This may involve the transfer of personal data to the USA.

Data collected often includes Instance IDs (advertising IDs with timestamps) that allow events to be linked but do not identify specific users. We do not personalize this data. Identifiers for mobile devices (AAID/IDFA) and cookie-like technologies are used.

Firebase helps us analyze App stability, performance, and user interaction, including session counts and durations, OS versions, and device models.

More information:

<https://support.google.com/firebase/answer/6318039?hl=en>

<https://policies.google.com/privacy/frameworks?hl=en>

You can disable ad identifiers via device settings:

Android: Settings > Google > Ads > "Reset advertising ID" or "Opt out of personalized ads"

iOS: Settings > Privacy > Advertising > "Limit Ad Tracking" or "Reset Advertising Identifier"

More info: <https://firebase.google.com/support/privacy>

## Information Sharing

We share your data only with selected third parties under strict safeguards to ensure data security and appropriate protection levels. Specifically:

- Subcontractors: We transmit personal data to a technical service providers located in Switzerland for contract performance or related purposes. This is always carried out on the basis of a data processing agreement in accordance with the provisions of the GDPR (legal basis: Article 6(1)(b) or (f) GDPR). The EU recognizes Switzerland as having adequate data protection.
- Government agencies: We may share information with public bodies where required by law, e.g., during legal investigations or court orders (Art. 6(1)(c) or (e) GDPR).

For the avoidance of doubt, we do not sell personal data to third parties for advertising purposes.

## Changes to This Privacy Policy

We reserve the right to amend this privacy policy in line with legal changes, new technologies, or updates to our tools and data processing practices. The current version is always available at <https://spt-payments.com/de-de/> under "Terms & Privacy."

## Data Retention and Deletion

We store data only as long as necessary to fulfill the intended purpose (full use of the App). 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](mailto: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. Our competent authority is the Austrian Data Protection Authority ([dsb@dsb.gv.at](mailto:dsb@dsb.gv.at), Address: Barichgasse 40-42, 1030 Vienna, Austria).