Privacy policy for the SocialCard (Version 20.06.2024)

General information

As the publisher of the SocialCard, we take the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with the statutory data protection regulations and in particular the EU General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG) as well as this privacy policy. This privacy policy explains what data we collect and what we use it for. It also explains how and for what purpose this is done. We would like to point out that data transmission over the Internet (e.g. when communicating by e-mail) may be subject to security vulnerabilities. Complete protection of data against access by third parties is not possible.

Wer ist verantwortlich für die Verarbeitung?

In accordance with the contractual agreement pursuant to Art. 26 GDPR, the:

- **secupay AG**
Goethestraße 6
01896 Pulsnitz
E-Mail: app@secupay.com

jointy with:

Paynetics AD
76, "James Bourchier" Blvd,
1407 Sofia
E-Mail: office@paynetics.digital

are responsible Persons.

secupay AG is the issuer of the SocialCard and, as a payment institution authorised by the German Federal Financial Supervisory Authority (BaFin), is responsible for the processes required to issue and load the cards. secupay AG is not an issuing office directly commissioned by Visa, but merely forwards the customer's data to the authorised offices and acts as an intermediary between the user and the licensed issuing office (card-issuing e-money institution).

Paynetics AD is the card-issuing e-money institution and offers registered users Visa debit cards and credit cards for use for payment at electronically connected acceptance points.

The parties work closely together when ordering, issuing and using the SocialCard. This also applies to the processing of your personal data. The parties have jointly determined the order in which this data is processed in the individual process stages. They are therefore jointly responsible for the protection of your personal data within the processing purposes described below.

Contact details of the data protection officer of secupay AG

Dominika Juszczyk
IBS data protection services and consulting GmbH
Zirkusweg 1, Hamburg, Deutschland
E-Mail: privacy@secupay.com

Contact details of the data protection officer of Paynetics AD

Paynetics AD
76A James Bourchier, Sofia, Bulgarien
dpo@paynetics.digital

How we collect your data?

Your data is collected when you provide it to us. This may be data that you provide to the person responsible for administration during the registration process or that you enter in the app. In addition, other data is automatically collected by our IT systems when you visit the app. This is primarily technical data (e.g. app version, operating system or timestamp of the app call). This data is collected automatically as soon as you start the app. As part of anti-money laundering measures and other legal obligations, your data may also be collected by third parties (e.g. KYC providers).

What we use your data for?

We process your personal data for the following purposes:

For the fulfilment of contractual obligations (Art. 6 para. 1 lit. b GDPR)

Personal data is processed as part of the performance of our contract with you as our customer or in order to take steps at your request prior to entering into a contract. This applies in particular to the use of the SocialCard and its functions, including processes for issuing and loading the card, for displaying the card payments made and the card balance, and for making payments with the SocialCard. Furthermore, your data is processed to generate a personal IBAN and for the technical and physical linking of the card with the personal data and the IBAN. This also includes communication with you. We use your personal information to communicate with you, e.g. by e-mail, regarding your concerns.

Relevant personal data may include in particular:

- Personal data (name, date of birth, place of birth, nationality and comparable data)
- Contact data (address, e-mail address, telephone number and comparable data)
- Identification data (ID and registration data)
- Debit card data of the SocialCard
- Login data (user name/email and password)

As part of the balancing of interests (Art. 6 para. 1 lit. f GDPR)

If necessary, we process your data beyond the actual fulfilment of the contract to protect our legitimate interests or those of third parties, for example:

- Assertion of legal claims and defence in legal disputes
- Ensuring IT security and IT operations
- Prevention of criminal offences and fraud detection
- Error-free provision of the website and the secupay app
- Crash analyses.

Relevant personal data may include in particular:

- Personal data (name, date of birth, place of birth, nationality and comparable data)
- Contact data (address, email address, telephone number and similar data)

- technical data (e.g. app version, operating system or timestamp of the app call, crash logs, IP address, device model, referrer URL, host name of the mobile device, language and region).

Due to legal obligations (Art. 6 para. 1 lit. c GDPR)

As a payment and e-money institution, we are also subject to various legal obligations, i.e. statutory requirements (e.g. Payment Services Supervision Act, Money Laundering Act, tax laws) and banking supervisory regulations (e.g. BaFin). The purposes of processing include identity and age verification, fraud and money laundering prevention, the fulfilment of control and reporting obligations under tax law and the assessment and management of risks within the company.

Relevant personal data may include in particular:

- Personal data (name, date of birth, place of birth, nationality and comparable data)
- Account and credit card data
- Sanctions list / money laundering prevention data

Use of Apple Pay

If you activate and use Apple Pay, you agree that we authorise Mastercard or VISA to transmit data such as first name, surname, PAN and expiry date to Apple for payment processing.

This data is transmitted to Apple in encrypted form. Apple decrypts the data, determines the card's payment network and encrypts the data again with a key that can only be decrypted by the payment network. Apple retains anonymised transaction data, including the approximate purchase amount, the name of the app developer and the app, the approximate date and time and whether the transaction was successfully completed.

Use of Google Pay

If you activate and use the widget for Google Pay, you agree that we authorise Mastercard to transmit data such as name, address, telephone number, sales data (e.g. merchant name, location, amount) to Google LLC for payment processing.

Who receives your data?

Within the company, those departments that need your data to fulfil our contractual and legal obligations will have access to it. Service providers and vicarious agents employed by us may also receive data for these purposes if they comply with banking secrecy and our written instructions under data protection law.

If you activate Apple Pay or Google Pay, we will authorise Mastercard or VISA to transmit your data to Apple Inc. or Google LLC for payment processing.

We pass on your data to Google LLC (Google Firebase and Google CrashLytics) to ensure the error-free provision of the secupay app and to carry out crash analyses.

We may only pass on information about you if this is required by law, if we are authorised to provide bank information and/or if processors commissioned by us guarantee compliance with banking secrecy and the requirements of the GDPR/BDSG. Under these conditions, recipients of personal data may be, for example:

- Joint controller (Paynetics AD)
- Processor (Publk GmbH)
- Administrator of the social card (e.g. public authority, employer)
- Other third parties (e.g. Deutsche Bundesbank, BaFin, European Banking Authority, European Central Bank, financial authorities, Federal Central Tax Office) if there is a legal or official obligation.

Is data transferred to a third country?

Data will only be transferred to countries outside the EU or the EEA (so-called third countries) if this is necessary for the execution of your orders (e.g. payment orders) or for the error-free provision of the secupay app (Google Firebase/CrashLytics).

The data transfer takes place on the basis of an adequacy decision or on the basis of an exception pursuant to Art. 49 para. 1 lit. b) GDPR.

Time limits for storage

In order to guarantee the principle of storage limitation in accordance with Art. 5 para. 1 lit. e GDPR, we store personal data in a form that enables the identification of data subjects only for as long as is necessary for the respective legitimate purposes.

Your data will be stored for 10 years from the conclusion of the legal transaction due to commercial or tax regulations in accordance with § 147 AO, § 257 HGB. This also applies in the event of cancellation of the legal transaction. Further storage takes place for the assertion, exercise or defence of legal claims, e.g. in the case of unresolved tax, audit or administrative proceedings.

Personal data that we process for the assertion, exercise or defence of legal claims is generally deleted after 3 years (regular limitation period in accordance with Section 195 BGB); in certain cases (e.g. claims for damages), the limitation period is 10 years or 30 years from the date on which the claim arises in accordance with Section 199 BGB, whereby the maximum storage period is 30 years from the date of the damaging event.

However, if a payment was cancelled before the legal transaction was concluded, the retention period is only 6 months.

What rights do you have regarding your dat?

Right to Information

In accordance with Art. 15 GDPR, you have the right to request confirmation from us as to whether personal data concerning you is being processed. If this is the case, you have the right to information in accordance with Art. 15 para. 1 GDPR, including a copy of your data in accordance with Art. 15 para. 3 GDPR, provided that the rights and freedoms of other persons are not affected. This includes business secrets, intellectual property rights or copyrights. The right to information can be restricted or refused in accordance with Section 34 BDSG. In this case, we will inform you of the reasons for the refusal.

Right to Rectification

In accordance with Art. 16 GDPR, you have the right to obtain from us without undue delay the rectification of inaccurate personal data concerning you and, depending on the purpose of the processing, the completion of incomplete data. Unless this is impossible or involves a disproportionate effort, we will inform all recipients to whom we have disclosed your personal data of the correction. According to Art. 19 S. 2 GDPR, you have the right to be informed about these recipients.

Right to Cancellation

In accordance with Art. 17 GDPR, you have the right to demand that we erase personal data concerning you without undue delay. We are obliged to erase your data if one of the reasons pursuant to Art. 17 para. 1 GDPR applies. If we have made your personal data public and are obliged to erase it, we will take reasonable steps pursuant to Art. 17 (2) GDPR to inform other controllers if you have requested the erasure of all links to this data or of copies and replications.

Unless this is impossible or involves a disproportionate effort, we will inform all recipients to whom we have disclosed your personal data of the erasure. Pursuant to Art. 19 S. 2 GDPR, you have the right to be informed about these recipients.

The right to erasure does not exist in accordance with Art. 17 para. 3 GDPR if the processing of your personal data is necessary for the reasons stated therein. This applies in particular if the storage of your data is still required due to legal storage obligations (Art. 17 para. 3 lit. b GDPR) or your data is required for the assertion, exercise or defence of legal claims (Art. 17 para. 3 lit. e GDPR).

The right to erasure also does not exist in accordance with Section 35 (3) BDSG if the storage of your data is required due to statutory or contractual retention obligations. In addition, the right to erasure may also be restricted in accordance with Section 35 (1) BDSG. In this case, the processing of your data is restricted in accordance with Art. 18 GDPR.

Right to Restriction of Processing

In accordance with Art. 18 GDPR, you have the right to demand that we restrict processing if one of the conditions specified therein is met.

If the processing of your data has been restricted, your data will continue to be stored in accordance with Art. 18 para. 2 GDPR, but will only be processed in another way if you consent to this or if this is done for the assertion, exercise or defence of legal claims, for the protection of the rights of another natural or legal person or for reasons of an important public interest of the EU or a member state.

If your data has been restricted, you will be notified before the restriction is lifted. Unless this is impossible or involves a disproportionate effort, we will inform all recipients to whom we have disclosed your personal data of the restriction. According to Art. 19 S. 2 GDPR, you have the right to be informed about these recipients.

Righ of Data Portability

Pursuant to Art. 20 GDPR, you have the right to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and you have the right to transmit those data to another controller without hindrance from us, where the processing is based on your consent pursuant to Art. 6(1)(a) GDPR or on a contract pursuant to Art. 6(1)(b) GDPR and the rights and freedoms of other natural persons are not adversely affected.

Right to Object

In accordance with Art. 21 GDPR, you have the right to object to the processing of your personal data at any time for reasons arising from your particular situation, provided that this is done on the basis of our legitimate interest in accordance with Art. 6 para. 1 lit. f GDPR. The right to object pursuant to Art. 21 (1) GDPR does not apply if we can demonstrate that we have legitimate grounds for the processing which override your interests, rights and freedoms or if the processing is necessary for the establishment, exercise or defence of legal claims. Irrespective of this, you have the right under Art. 21 para. 2 GDPR to object at any time to the processing of your data for the purpose of direct marketing, including profiling in connection with direct marketing. In this case, we will no longer process your data for the purpose of direct marketing.

Automated decision-making pursuant to Art. 22 GDPR

In accordance with Art. 22 (1) GDPR, you have the right not to be subject to a decision based solely on automated processing - including profiling - which produces legal effects concerning you or similarly significantly affects you.

Right to submit a complaint pursuant to Art. 77 GDPR

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority pursuant to Art. 77 GDPR if you consider that the processing of your personal data infringes the GDPR. You can contact any supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, including the supervisory authority responsible for us:

Saxon Data Protection Officer
Devrientstraße 5
01067 Dresden
Telefon: 0351/85471 101
Telefax: 0351/85471 109
Internet: www.datenschutz.sachsen.de
E-Mail: saechsdsb@slt.sachsen.de