Privacy Policy for cardholders, according to Art. 14 GDPR

Preamble

We take the protection of personal data and thus your privacy very seriously. At this point, we would like to outline how we protect your data and what impact it has on you when using our personalized services. In order to ensure the greatest possible protection of your privacy, it goes without saying that we comply with all legal data protection provisions. We adhere to the provisions of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act New (BDSG new) due to the adaptation of data protection law to Regulation (EU) 2016/679 and the implementation of Directive (EU) 2016/680 (Data Protection Adaptation and Implementation Act EU DSAnpUG-EU).

1. Name and address of the controller

The controller and service provider is the EVO Payments International GmbH, Elsa-Brändström-Str. 10–12 ,50668 Cologne (hereinafter, referred to as "EVO").

2. Name and address of the Data Protection Officer

Our data protection officer is Dr. Karsten Kinast, KINAST Rechtsanwaltsgesellschaft mbH, Hohenzollernring 54, 50672 Cologne. You can contact our data protection officer at any time for any questions concerning data protection, preferably by e-mail to: Evo@kinast-partner.de or in writing to: EVO Payments International GmbH, Elsa-Brändström-Str. 10–12, 50668 Cologne (please state in the subject line "EVO Data protection").

3. Personal data

Personal data means any information relating to an identified or identifiable natural person. This includes your name, email address, or account information.

4. Processing of personal data

EVO processes the data required for safe, efficient and reliable execution in the context of cashless payment transactions:

- Handling of cashless payment transactions (transaction processing) in stationary and e-commerce areas. Depending on the chosen payment method, this includes the transaction data, such as IBAN, card number, card expiration date and card sequence number, date, amount, time, identification of the respective card reader and the test data of your card-issuing bank;
- anti-fraud and prevention measures to prevent loss of payment in individual cases;
- credit check for dynamic payment control: This is done immediately and only for the duration of transaction processing, in particular by checking and validating account, card and address data as well as IP addresses with regard to their plausibility;
- protection of your own IT infrastructure and detection and tracking of cyber attacks: This is for example done, by temporarily storing IP addresses for fault and fault detection;
- summary of claims across specific billing cycles to simplify payment processes and optimize costs.

5. Legal basis for processing

The legal basis of the processing is primarily Art. 6 Par. 1 lit. b) GDPR. The processing of the above personal data is necessary for the execution of the respective main contract between cardholder and merchant, in order to fulfill the payment order.

Further processing is justified by the overriding legitimate interests of EVOs, Art. 6 para. 1 lit. f) GDPR, in particular to protect against fraud or to minimize the risk of payment defaults.

In addition, EVO is subject to legal regulations and regulations of cashless payment transactions, in particular to prevent fraud and misuse. Furthermore, there are tax and commercial storage requirements of 6 or 10 years for accounting-related data. The legal basis of the processing is Art. 6 Par. 1 lit. b) GDPR.

6. Origin of personal data

EVO receives your data by transfer to authorized dealers to process the payment instructions either through their online shops or through card readers provided by EVO (so-called POS terminals).

7. Recipient of personal data

These data will also be transmitted to the following categories of recipients where necessary, to implement the contracts, as well as to fulfill legal obligations and to protect our legitimate interests:

> Banks, Card Schemes (including Visa Europe, Mastercard);
> E-commerce service provider (so-called payment service provider "PSP", provider of payment solutions for online shops);
> Authorities (especially investigating authorities such as police and prosecutors) in the case of justified information requests.

8. Processing in countries outside the European Economic Area

Transfers by EVO to recipients in so-called third countries outside the European Union / European Economic Area shall take place if and to the extent necessary, for the above mentioned purposes. An appropriate level of data protection is ensured, either by an adequacy decision of the EU Commission, by the inclusion of appropriate contractual clauses or because the requirements of Art. 49 GDPR have been met.

9. Storage time

Personal data will be deleted unless one of the following exceptions applies, after the contractual or legal purpose of their storage no longer exists:

> Fulfillment of commercial and tax law as well as other storage obligations (e. g., storage of accounting-relevant data for 10 years in accordance with § 147 AO);
> Preservation of evidence, in accordance with the statute of limitations as stipulated by law.

10. Measures of automated decision-making / profiling / scoring

EVO does not perform any automated decision-making / profiling / scoring measures. The decision on which payment and verification types are offered is based on transaction-specific amount limits. Data of the cardholder is not taken into account.

11. Data security

We take technical and organizational security measures to protect your data as comprehensively as possible against unwanted access.

12. Your rights as a data subject

12.1 Right to Information

You have the right to request information from us at any time on the data stored about you, as well as on the source, recipients or categories of recipients to whom this data is passed on and on the purpose of storage.

12.2 Right to Withdraw

If you have given consent to the use of data, you can withdraw it at any time, without stating reasons and effect for the future.

12.3 Right to Rectification

If your stored data is inaccurate, you can always contact us and have it corrected.

12.4 Right to Erasure and to Restriction of Processing

You have the right to have the data stored about you deleted and restricted. The deletion of your personal data is usually carried out, within two working days, after claiming data subject right. If the deletion is contrary to legal, contractual or tax-law or commercial-law retention obligations or other legal requirements, the processing of your data can only be restricted. It is not possible to to provide information, after your data has been deleted..

12.5 Right to Data Portability

If requested, we will provide you or another controller with the data in a structured, common and machine-readable format to the extent that it is technically feasible.

12.6 Right to Object

You have the right to object to the data processing, at any time, and without giving reasons. It may be possible that the contractwith your in this case, the contract with your Merchant is not feasible any longer.

12.7 Contact for claiming data subjects rights

Please refer to clause 1 and 2 in this privacy statement in order to claim your rights.

12.8 Right to lodge a complaint with the supervisory authority

You have the right to contact the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, Kavalleriestr. 2–4, 40213 Düsseldorf (poststelle@ldi.nrw.de) to file a complaint against the processing of your personal data, if you see yourself violated in your data protection rights.