Privacy Policy pursuant to Art. 13, 14 GDPR

for the app „TransactVerify“, version V[2.0]

This English translation is for information purposes only. In case of inconsistencies between the German and the English version of this document the German version shall prevail. The German version can be found here: [https://www.fiserv.com/en-de/transact-verify/datenschutzerklarung.html].

The institution that issued your (credit or prepaid) card ("**Card Issuer")** hereby informs you about the processing of your personal data (Art. 4 No. 2 General Data Protection Regulation ("**GDPR"))** by the Card Issuer and the rights to which you are entitled under data protection law in connection with the App "TransactVerify" ("**App**“). The Card Issuer is your bank or other institution with which a contract for your card exists - either directly with you or, if you received the card from your employer, with your employer ("**Card Contract**").

The App allows you to

a) authenticate for internet payment transactions ("**Internet Payments**") through Mastercard® Identity Check™ ("**3D Secure**"). 3D Secure is a process that aims to make Internet Payments more secure by verifying your identity during the checkout process. The authentication allows you to identify yourself as an authorized cardholder to the Card Issuer. 3D Secure thus serves to prevent abusive transactions;

b) view and download card statements for a card (functional area "**EStatements**") that you have registered in the App, if the Card Issuer offers this functionality;

c) view information about transactions made with a card that you have registered in the App (functional area "**Transactions**"), provided that the Card Issuer offers this functionality;

d) receive notifications in the App when transactions have been made with a card that you have registered in the App (functional area "**Alert Service**"), provided that the Card Issuer offers this functionality;

e) view of the card limit and the potentially remaining amount for the month in question for a card that you have registered in the App (functional area "**Card Balance**").

This privacy policy pursuant to Art. 13, 14 GDPR for the App supplements the privacy policy (or data protection information) of the Card Issuer for the Card Contract, which you can obtain from the Card Issuer.

1. Who is responsible for data processing and who can I contact?

The data controller is the Card Issuer.

The Card Issuer's data protection officer can be reached using the contact details provided by the Card Issuer in the privacy policy or the data protection information for the Card Contract.

2. What data is used and what are the sources of the data?

2.1 When you register for the App using 3D Secure,

a) you choose a PIN that will allow you to authenticate yourself when making Internet Payments in the future (3D Secure);

b) you also have the option of choosing biometric recognition to authenticate yourself for Internet Payments in the future (3D Secure). If you have selected this option, the App will ask the mobile device on which you downloaded the App whether biometric mode has been activated. If it has not yet been activated, the mobile device notifies the App accordingly. Once you've enabled biometric mode in your mobile device's settings and the device has successfully captured your fingerprint (touch ID) or facial recognition (face ID), the device will notify the App that the biometrics are correct. In the settings of the mobile device, you decide whether you choose facial recognition (face ID) or fingerprint recognition (touch ID). The face ID and/or fingerprint is only stored on your mobile device, it is not transmitted to the App;

c) you enter your card number in the App, either manually or by scanning the card. When you enter your card number by scanning the card, you allow the App to use the mobile device's camera;

d) the App establishes a connection between the card number you enter in the App and the App installation number on your mobile device ("**EmCertID**");

e) the App collects the operating system and the type of your mobile device;

f) you choose a preferred method to obtain an identification code for the authentication process required during registration. You can choose to have it transmitted by SMS, 1 cent transaction or letter.

If you have chosen to receive the code by SMS, you will also enter the last four digits of your bank details, the expiration date of your card, your date of birth and your mobile phone number in the App.

Once you have received the identification code via your chosen method, you enter the identification code in the App.

If possible, your data will be processed in encrypted form.

2.2 If you are asked to authenticate yourself using 3D Secure when making an Internet Payment,

a) the Card Issuer will send you a message on your mobile device using the card number and EmCertID. This message contains the last four digits of your card number, the name of the merchant and/or acceptance point where the Internet Payment is made, as well as the date, time and amount of the Internet Payment;

b) the App captures the operating system and type of your mobile device;

c) you confirm
   (i) the payment either by entering the PIN you have chosen or by the biometric recognition method you have chosen. When you use biometric recognition, biometric recognition is performed by your mobile device, and the app only informs whether the authentication was successful or not. Your Face ID or Your fingerprint will not be transmitted to the App;

   (ii) or, alternatively, if you have chosen the offline authorization function on the merchant's website (or the acceptance point) to approve the payment, you open the QR code scanner in the App and scan the QR code displayed on the merchant's website to confirm the payment;

d) or, if you do not want to confirm the transaction, decline it.

As far as possible, your data will be processed in encrypted form.

2.3 If the "Transactions" functionality is offered by the Card Issuer, the App allows you to view all transactions you have made with the Card, regardless of where the transactions were made (e.g. on the Internet, in physical stores or cash withdrawals). The display includes the last four digits of your Card number, the name and (if provided by Mastercard) the address and additional information about the merchant/acceptance point where the transaction was made, the date and time of the transaction, the transaction amount in EUR and, if applicable, in foreign currency with exchange rate and currency conversion fee, and the total amount of all transactions. This data is provided by the Card Issuer (via MasterCard if applicable).

2.4 If you are offered the "EStatement" functionality by the Card Issuer and you have activated the feature in the App, you will be given access to your card statements with information about the transactions you have made with the card. You can also download the card statements as a pdf document. The card statements contain a subset of the data described in clause 2.3 and are provided by the card Issuer.

2.5 Using the "Card Balance" function, you can view the limit (the credit limit) as well as the limit for the card that is still available, i.e. not yet used for payments (e.g. Internet Payments, payments in physical stores or cash withdrawals) for the month in question. This information become provided by the card Issuer.

2.6 If your card Issuer offers you the "Alert Service" functionality and you have agreed to receive push notifications for the App in your mobile device's power settings, you will receive a message in the App after a payment has been made with a card. This applies to all transactions, regardless of whether they are e.g. Internet Payments, payments in physical stores or cash withdrawals. The notification contains the last 4 digits of your Card number, the amount and the currency of the transaction. The notification is provided by the Card Issuer.

2.7 Location of data
   a) Cards registered in the App and related data (Card number, EStatements, transaction data) are generally stored on a server outside the App and mobile device and only retrieved from the server into the App if and as long as the App is open. When the App is closed again, the data is not stored in the App, but is discarded.
   b) Data which is saved in the App
      (i) Data which is used in the registration process;
      (ii) Data which is required for the operation of the App (e.g. PIN to confirm Internet Payments) and not connected to the card;

Card numbers are only partially displayed (masked).

Only the data that is required for the operation of the App (e.g. PIN to confirm Internet Payments) and not connected to the Card will be stored on the mobile device on which the App was downloaded.

Data used for the registration process is stored in the App.

3. What does the Card Issuer process your data for (purpose of processing) and on what legal basis?

The Card Issuer processes your personal data for the following purposes and on the following legal basis:

3.1 For the fulfilment of contractual obligations (Art. 6 para. 1 letter b GDPR): If the Card Contract exists between the Card Issuer and you, the processing of personal data is carried out for the purpose of fulfilling the Card Contract for the purpose of carrying out your transactions.

3.2 In the context of a balancing of interests (Art. 6 para. 1 (f) GDPR)**:** If the Card Contract exists between the Card Issuer and your employer, the processing of personal data is carried out to protect your legitimate interests as well as those of your employer (e.g. Card statements and transaction overviews for company credit Cards).

3.3 Due to legal requirements (Art. 6 para. 1 lit. c GDPR) or in the public interest (Art. 6 para. 1 lit. e GDPR): In addition, the Card Issuer is subject to legal obligations, i.e. legal requirements (e.g. from the Payment Services Supervision Act (ZAG)) and regulatory requirements (e.g. the Federal Financial Supervisory Authority (BaFin)). The purposes of the processing include, among other things, the verification of your identity for Internet Payments and the increase of security in online payment transactions as well as the reduction of fraud risks.

3.4 Art. 25 para. 2 sentence 2 TTDSG: With regard to the technology that accesses your mobile device, the legal basis is Art. 25 para. 2 sentence 2 Telecommunications-Telemedia-Data Protection Act (TTDSG). This technology is required to meet the legal and regulatory requirements for fraud prevention in payment transactions.

4. Who gets my data?

4.1 The Card Issuer provides access to those departments that need your data to fulfil the Card Issuer's contractual, legal and regulatory obligations.

4.2 The processors used by the Card Issuer (Art. 28 GDPR) may also receive data for these purposes. These are the following processors pursuant to Art. 28 GDPR:

- First Data GmbH, 61348 Bad Homburg (insofar as First Data GmbH is not the Card Issuer itself, but acts as a service provider for another Card Issuer) ("**FIRST DATA**");
- Netcetera AG, 8040 Zurich, Switzerland: Operation of the authentication server for 3D Secure or the server for the App ("**Netcetera**");
- Deutsche Telekom Business Solutions GmbH, 53227 Bonn: Sending SMS for registration in the App.

4.3 Other recipients outside of the Card Issuer may receive information about you, if legal provisions or regulatory requirements allow or require this, if this is necessary for the performance of the Card Contract or if you have consented. Under these conditions, recipients of personal data may be, for example: Public bodies and institutions (e.g. Deutsche Bundesbank, Federal Financial Supervisory Authority (BaFin), tax authorities, Money Laundering Reporting Offices, Investigative Authorities, Central Office for Financial Transaction Investigations (FIU)) in the event of a legal or regulatory obligation.

5. How long will my data be stored?

5.1 Data associated with the Card (Card number, transaction data, EStatements) is not stored in the App, but on a server outside the App and mobile device, and is only retrieved from the server to the App if and as long as the App is open. This data is stored as long as the Card is an active Card, i.e. it is not cancelled and is not permanently blocked.

5.2 Data related to 3D Secure authentication during an Internet Payment is stored for 13 months.

5.3 Data used to operate the App that is not connected to the Card and is not used for authentication (see previous paragraphs) will be stored in the App as long as the App is active, i.e. not deleted from the mobile device.

5.4 Data used for the registration process will be stored in the App and deleted after 30 days, unless it is data mentioned in the preceding paragraphs.

6. Is data transferred to a third country or to an international organization?

6.1 A transfer of personal data to third countries (countries outside the European Economic Area ("**EEA**")) only takes place if an adequate level of data protection has been confirmed to the third country by the EU Commission or other appropriate data protection guarantees (e.g. binding corporate rules or EU standard contractual clauses) have been agreed or you have given your consent to the Card Issuer.

6.2 Your personal data will be processed outside the EEA in Switzerland by Netcetera. For Switzerland, the EU Commission has issued an adequacy decision under data protection law. In addition, First Data and Netcetera have contractually agreed on the EU Standard Contractual Clauses.

6.3 Netcetera uses subcontractors outside the EEA in North Macedonia who may also process your personal data. Netcetera has contractually committed itself to First Data in the EU Standard Contractual Clauses to contractually agree on suitable safeguards for the transfer of personal data outside the EEA in accordance with Article 44 et seq. GDPR.

7. What data protection rights do I have?

Every affected subject has the right for information pursuant to Art. 15 GDPR, the right to rectification pursuant to Art. 16 GDPR, the right to erasure pursuant to Art. 17 GDPR, the right to restriction of processing pursuant to Art. 18 GDPR and the right to data portability pursuant to Art. 20 GDPR. The right to information and the right to erasure are subject to the restrictions set out in Sections 34 and 35 of the Federal Data Protection Act (BDSG).

In addition, there is a right to lodge a complaint with the data protection supervisory authority of your federal state (Art. 77 GDPR in conjunction with §19 BDSG).

You can reach the Card Issuer's data protection officer using the contact details provided by the Card Issuer in the privacy policy or the data protection information for the Card Contract.

8. Is there an obligation for me to provide data?

You only need to provide the personal data that is necessary for the operation of the App and your authentication using 3D Secure. Without this information, the Card Issuer may have to decline an Internet Payment, especially if you do not use an alternative method of authentication for Internet payments offered by the Card Issuer.

The EStatements, transactions and Alert Service functionalities, on the other hand, are optional.

9. To what extent is there automated decision-making in individual cases?

Automated decision-making does not take place.

10. To what extent is my data used for profiling (scoring)?

The Card Issuer processes some of your data automatically with the aim of evaluating certain personal aspects (profiling). Due to legal and regulatory requirements, the Card Issuer is obliged to ensure that an Internet Payment is made by the rightful Cardholder and must therefore authenticate the Cardholder. Data evaluations are also carried out. These measures also serve to protect you.

Information about your right to object in accordance with Art. 21 GDPR

You have the right to object, on grounds relating to your particular situation, at any time to the processing of personal data concerning you that is carried out on the basis of Article 6(1)(f) of the GDPR (data processing based on a balancing of interests); this also applies to profiling based on this provision within the meaning of Art. 4 No. 4 GDPR.

If you object, the Card Issuer will no longer process your personal data unless it can demonstrate compelling legitimate grounds for the processing that outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.