Data protection information in accordance with Art. 13, 14 GDPR
for the app "TransactVerify"

The issuer (the "**Issuer**") of your (credit or pre-paid) card (the "**Card**") hereby informs you about the processing of your personal data (Art. 4 No. 2 General Data Protection Regulation (the "**GDPR**")) by your Issuer and the rights to which you are entitled under data protection law in connection with the app "TransactVerify".

The App enables you to

(i) authorize (approve) or decline e-commerce transactions you make with your Card (the "**Transactions**") (function "3D Secure" (Mastercard® Identity Check)). The 3D Secure procedure increases the security of Card payments on the internet and serves to reduce the risk of fraud by only executing payment transactions after the cardholder has been authenticated;

(ii) get an overview over past and current Card statements (function "eStatements"),

(iii) get an overview over all Transactions made with your Card (function "Card balance"),

(iv) enable real-time push-notifications for every Transaction, and

(v) get current information on the Card's limit.

The Issuer of the Card is your bank or other institution with whom a contract regarding your Card exists - either with you directly or, in case you have been provided with the Card by your employer, with your employer (the "**Card Contract**").

This data protection information in accordance with Art. 13, 14 GDPR for the app TransactVerify" (the "**App**") amends the Issuer's data protection information for the Card Contract, which you can receive from the Issuer (the "**Issuer's Card Contract Data Protection Information**").

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

The controller is the Issuer.

The Issuer's data protection officer can be contacted at the contact data notified to you in the Issuer's Card Contract Data Protection Information.

2. What are the data and the sources of the data?

2.1 When you register for the App via 3D Secure (Mastercard® Identity Check™),

a) you choose a PIN which you may use in order to authenticate yourself during future internet Card payments;
b) you have in addition the ability to choose biometric recognition in order to authenticate yourself during future internet Card payments. If you have selected this option, the App asks the mobile device on which you have downloaded the App whether the biometrics mode has been enabled. If it has not been enabled yet, the mobile device notifies the App accordingly. Once you have enabled the biometrics mode in the settings of your mobile device and the device has successfully collected your fingerprint or face-ID, the device notifies the App that the biometric data where correct. You determine in the settings of the mobile device whether you choose face-ID our touch-ID/fingerprint. The face ID and/or fingerprint will only be stored in your mobile device, it will not be transferred to the App.
c) you enter your Card number in the App, either manually or by scanning the Card. If you enter your Card number by scanning the Card, you approve the use of the camera on your mobile device on which you have downloaded the App;
d) a connection between the Card number you have entered in the App and the number of the App installation on your mobile device on which you have downloaded the App (the "**emCertID**") is collected;
e) also, the operating system and the type of your mobile device are collected. ;
f) you choose a preferred method to get an identification code for the authentication process necessary during the registration. You may either choose SMS, 1 cent Transaction or letter.
If you have chosen SMS in order to receive the identification code, you also enter the last four digits of your bank account number, the Card expiration date, your date of birth and your mobile phone number in the App.
Once you have received the identification code through your chosen channel, you enter the identification code in the App.

To the extent possible, your data are processed encrypted.

2.2 When you authorize/confirm a Transaction through 3D Secure (Mastercard® Identity Check™):

a) You receive a push message to your mobile device from the Issuer who uses your Card number and the emCertID. The push message contains your Card number (last four digits), the merchant's name and the date, time and amount of the Transaction in the chosen currency.
b) The operating system and the type of your mobile device are collected.
c) ;You authorize/confirm
   i. the Transaction either through entry of your chosen PIN or through your chosen biometric recognition method. If you authorize/confirm through biometric recognition, the biometric recognition is performed by your mobile device, and the App is only notified whether the

authentication was successful or not. Your face ID or fingerprint will not be transferred to the App.

ii. alternatively, if you have chosen the offline authorization function on the website of the merchant where you are about to make the Transaction, you open the QR code scanner in the App and scan the QR code displayed on the merchant's website to authorize/confirm the Transaction.

d) if you do not want to authorize/confirm the Transaction, you decline it

To the extent possible, your data are processed encrypted.

2.3 You may also view a list of all completed Transactions you have made, including: Card number (last four digits), merchant name, address (if provided by MasterCard), additional merchant information (if provided by MasterCard), Transaction date and time, Transaction amount in EUR and, if applicable, in foreign currency with the exchange rate and currency conversion fee, and total amount of all Transactions. These data are provided by the Issuer.

2.4 If the "eStatement" function is offered to you by the Issuer and you have activated the function in the App, you will get access to your Card statements with information on the Transactions you have completed, which Card statements you may also download as pdf documents. The Card statements contain a subset of the data described dunder clause 2.3 and are provided by the Issuer.

2.5 You may also view the limit of your Card including already used as well as the still available amount. The limit is provided by the Issuer.

2.6 If you have chosen to receive push-notifications for the App in the device settings of your mobile device, you will receive a push message whenever a Card you have previously registered in the App has been used for Transactions (function "Alert Service"). The notification contains the last 4 digits of your Card number, the amount and the currency.

2.7 Cards which have been registered in the App and data related to these Cards (e.g. Card number, Transactions, eStatements) are not stored in the App, but on a central server outside of the App and the mobile device. Each time the App is opened the Card data is retrieved from the server and discarded when the App is closed again. Card numbers are only partially displayed (masked).

In general, all data which is connected to the Card is saved on a server (e.g. Card number, Transactions) outside of the App and the mobile device. Only the data which is necessary to run the App (e.g. PIN in order to authorize/confirm Transactions) is saved on the mobile device on which the App has been downloaded.

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

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

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

3.1 For the fulfillment of contractual obligations (Art. 6 para. 1 letter b GDPR)

If the Card Contract exists between the Issuer and you, the processing of personal data takes place for the fulfillment of the Card Contract, e.g. the execution of your Transactions.

3.2 In the context of a balancing of interests (Art. 6 para. 1 letter f GDPR**)**

If the Card Contract is between the Issuer and your employer, personal data is processed to protect your legitimate interests, i.e. execution of Transactions and provision of eStatements, Transaction data, and Card limit data to you.

3.3 Due to legal requirements (Art. 6 para. 1 letter c GDPR) or in the public interest (Art. 6 para. 1 letter e GDPR)

In addition, the Issuer is subject to various legal obligations, i.e. legal requirements (e.g. from the Payment Services Supervision Act (ZAG)) as well as regulatory requirements (e.g. from the Federal Financial Supervisory Authority (BaFin)). The purposes of processing include identity checks. The Issuer pursues its legitimate interest in increasing the security in online payment transactions and the effective reduction of fraud risks.

3.4 Art. 25 para. 2 sentence 2 TTDSG

With regards with the regards to the technology which accesses your mobile device, the legal basis is Art. 25 para. 2 sentence 2 TTDSG. This technology is absolutely necessary in order to fulfil the legal and regulatory requirements for fraud prevention in payment transactions.

4. Who receives my data?

4.1 Within the Issuer, those departments that require your data to fulfill the Issuer's contractual and legal obligations will receive it.

4.2 Processors used by the Issuer (Art. 28 GDPR) may also receive data for these purposes.

These are the following data processors in accordance with Art. 28 GDPR:

- First Data GmbH, 61348 Bad Homburg (where First Data GmbH is not an Issuer itself, but acts as a service provider for the Issuer) ("**First Data**");
- Netcetera AG, 8040 Zurich, Switzerland: Operation of the authentication server for 3D Secure (Mastercard® Secure Code™ and the App ("**Netcetera**");
- Deutsche Telekom Business Solutions GmbH, 53227 Bonn: Sending of SMS for the registration in the App;

4.3 Information about you may be disclosed to other recipients outside the Issuer if this is permitted or required by law, if this is necessary for the performance of the Card Contract or if you have given your consent. 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, investigating authorities, Central Financial Transaction Investigation Unit (FIU)) in the event of a legal or official obligation;

5. How long will my data be stored?

Data which is connected to the Card (Card number Transactions, eStatements) isn't stored in the App, rather on a server and only retrieved from the server into the App if and as long as the App is opened.

This data is stored as long as the Card is an active Card (i.e. not terminated and not blocked). Data relating to 3D Secure authentication during a Card payment is stored for 13 months.

Data that is used to run the App and which is not connected to the Card (see previous sentences) is stored in the App as long as the App is active (i.e. not deleted from the mobile device).

Data which is used for the registration process is stored in the App and deleted after 30 days, unless it is data which is mentioned in the previous sentences.

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

Personal data will only be transferred to third countries (countries outside the European Economic Area (EEA)) if the third country has been confirmed by the EU Commission to have an adequate level of data protection or if other appropriate data protection guarantees (e.g. binding corporate rules or EU standard contractual clauses) have been agreed or if you have given your consent to the Issuer.

Your personal data is processed outside the European Union/European Economic Area in Switzerland at Netcetera. For Switzerland, an adequacy decision under data protection law by the European Commission is available. Furthermore, First Data and Netcetera have contractually agreed the EU Standard Contractual Clauses.

Netcetera uses subcontractors outside the European Union/European Economic Area in North Macedonia, which also may process your personal data. Netcetera has contractually committed itself to First Data in the EU Standard Contractual Clauses to contractually agree on suitable guarantees for the transfer of personal data outside the European Union/European Economic Area in accordance with Art. 44 et seq. GDPR.

7. What data protection rights do I have?

Every data subject has the right of access under Art. 15 GDPR, the right to rectification under Art. 16 GDPR, the right to erasure under Art. 17 GDPR, the right to restriction of processing under Art. 18 GDPR and the right to data portability under Art. 20 GDPR. The restrictions under Sections 34 and 35 of the German Federal Data Protection Act (BDSG) apply to the right of access and the right to erasure.

In addition, you have the right to lodge a complaint with the data protection supervisory authority in your federal state (Art. 77 GDPR in conjunction with Section 19 BDSG).

You can contact the Issuer's data protection officer at the contact data notified to you in the Issuer's Card Contract Data Protection Information.

8. Do I have an obligation to provide data?

You only need to provide the personal data that is required for operating the App and authorization/confirmation of Transactions through 3D Secure (MasterCard® Identity Check).

9. To what extent will my data be used for profiling (scoring)?

The Issuer processes some of your data automatically with the aim of evaluating certain personal aspects (profiling). Due to legal and regulatory requirements, the Issuer is obliged to ensure the Transaction is initiated by the rightful cardholder and therefore has to authenticate the cardholder. Data is analyzed in the process. These measures also serve to protect you.

Information about your right to object in accordance with Art. 21 General Data Protection Regulation (GDPR)

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (f) of Article 6(1) GDPR (data processing on the basis of a balancing of interests); this also applies to profiling based on this provision within the meaning of Article 4(4) GDPR, which your Issuer uses to assess creditworthiness.

If you object, your Issuer will no longer process your personal data unless your Issuer can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.