# INFORMATION TO CUSTOMERS OF COMPUTOP WHO ARE CONTROLLERS ACCORDING TO THE GENERAL DATA PROTECTION REGULATION (GDPR) ON QUESTIONS RELATED TO DATA PROTECTION LAW WHEN USING THE 3D-SECURE 2.0 PROCEDURE

*- Please note that the purpose of this information sheet is merely to provide the merchant, as the one who is legally responsible under data protection law, and his data protection officer with a guideline for carrying out his own essentially necessary case-related legal assessment, as well as for creating a wording of the data protection information. We would also like to point out that - although the contents of this information sheet have been researched with greatest care - no liability can be accepted for the accuracy, completeness and currentness of the information. -*

## A. GENERAL INFORMATION ON 3D-SECURE 2.0, PROCESS FLOW

3D-Secure 2.0 (hereinafter: 3DS 2.0) is a worldwide standard of the card networks (Visa, MasterCard, JCB, Diners, AMEX etc.), developed by EMVCo, an association of card networks.

Details of the 3DS 2.0 procedure can be found in the latest version of the "EMV 3-D Secure Protocol and Core Functions Specification" (hereinafter "EMV Spec", linked in footnote[1]) of EMVCo.

3DS 2.0 is one of the procedures by which the strong customer authentication[2] as laid down in the EU Directive 2015/2366 (Payment Services Directive 2, PSD 2) is being realized. In Germany, PSD 2 has been implemented within the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz, ZAG). By using the 3DS 2.0 procedure, it will be confirmed that the person initiating an eCommerce transaction is also entitled to use the respective payment card.

The transition of the 3DS procedure from version 1.0 to version 2.0 currently raises data protection questions with numerous merchants, understandably. We have therefore researched some information for you and compiled it in this information sheet. Background of the general uncertainty on this subject is that with the application of the new 3DS 2.0 procedure, merchants are potentially also sending along up to 100 transaction- and customer-related data elements which origin, inter alia, from the contractual relationship between the merchant and the buyer (e.g. shipping address or billing address), or from the buyer's customer account at the merchant, or which can be derived from the latter (e.g. data on the buyer's use of the account, such as the duration of the account's existence or the frequency of password changes). Within the 3DS 2.0 procedure, the respective data elements are being sent to the issuer, i.e. to the card-issuing bank of the respective card by which payment is about to be made.

While the 3DS 1.0 procedure had always required an interaction of the buyer (such as a password or PIN entry) and therefore had needed much fewer data elements, now for the 3DS 2.0 procedure, numerous additional data elements were implemented in order to allow a so-called "frictionless flow"[3] in which no interaction of the cardholder is required during the authentication procedure.

The authentication procedure of 3DS 2.0 includes two verification levels: at the first verification level it is being checked whether a "frictionless flow" is possible due to the additional data elements provided by the merchant. If the authentication procedure at the first verification level comes to the result that a "frictionless flow" is not possible, the so-called "challenge flow"[4] will be executed at the second verification level which additionally requires an interaction of the cardholder (query of a second factor such as a password or PIN entry).

Meaning and purpose of the frictionless flow are, after all, to increase the usability, to increase conversion rates and to prevent early purchase cancellations. The more data elements a merchant will be sending, the higher the likelihood that a frictionless flow will be possible.

The individual data elements for the entire 3DS 2.0 procedure can be found in the latest version of the EMV Spec[5]. Some of these data elements are mandatory to perform the 3D Secure 2.0 process, some are conditionally mandatory (i.e. mandatory under certain conditions), and some are optional. Among the conditionally mandatory data elements in the EMV Spec are also some which are marked "required (if available) unless market or regional mandate restricts sending this information".

The conditionally mandatory and optional data elements are those for which the merchant needs to assess whether there are reasons (in particular legal reasons) for which the data elements cannot be sent along. For the aforementioned categories of data elements, a case-related assessment of the merchant together with his data protection officer is necessary.

## B. LEGAL IMPLEMENTATION OF DATA PROTECTION ASPECTS IN CONNECTION WITH 3DS 2.0

There are various possibilities to legally implement the use of 3DS 2.0 in terms of data protection law:

**Alternative 1:**

**Based on statutory permissions**

For sending along the up to 100 transaction and customer-related data elements, at first some statutory permissions can be assessed.

To our opinion, Article 6 section 1 sentence 1 lit. b, c and f GDPR can be considered (for details resp. a guideline for the assessment, see below C under "Purposes for which personal data is intended to be processed and legal basis for the processing"). At this point, in any case a case-related assessment by the merchant and his data protection officer is necessary, individually for all data elements, which may also come to the conclusion that some of the data elements cannot be sent along.

In order to fulfil the statutory data protection information obligations according to Articles 13 and 14 GDPR when the processing will be based on statutory permissions, the relevant data protection information (see below for details) should, as far as possible, be included directly at the check-out as well as into the data protection statement on the merchant shop's website. To our optinion, the information at the check-out can also be summarized with a link to the data protection statement, which then contains the complete information. The more transparent the data processing will be for the customer at the end, the better!

**Alternative 2:**

**Incorporation into the contract**

Optionally, information about 3DS 2.0 together with all information required by data protection law according to Articles 13, 14 GDPR (see below), can also be included in the merchant's general terms and conditions on which the contract with the end customer is based. In our view, this is not absolutely necessary, but would have the advantage that Article 6 section 1 sentence 1 lit. b GDPR ("necessity for the performance of a contract") could presumably be used as the legal basis entirely for all data elements (in the sense of Article 13 section 2 lit. e GDPR, the provision of personal data would then be "a contractual requirement"). The choice of this alternative is particularly useful if the case-related legal assessment of alternative 1 should have led to the conclusion that there are doubts regarding the lawfulness of the processing of individual data elements when based on statutory permissions.

Additionally, we recommend to also include the data protection information according to Articles 13, 14 GDPR into the check-out and into the data protection statement of the merchant shop's website (at the check-out possibly summarized, see note at alternative 1).

**Alternative 3:**

**Obtaining of consents according data protection law**

Alternatively, if the legal assessment under alternative 1 reveals that there are doubts regarding the lawfulness of the processing of individual data elements when based on statutory permissions, it may also be considered, as a precautionary measure, to obtain a declaration of consent from the buyer at the check-out pursuant to Article 6 section 1 sentence 1 lit. a GDPR together with the data protection information according to Article 13, 14.

In addition, we recommend to also include the information according to Articles 13, 14 GDPR into the data protection statement of the merchant shop.

## C. COMPLIANCE WITH THE DATA PROTECTION INFORMATION OBLIGATIONS ACCORDING TO ARTICLES 13, 14 GDPR

According to the stipulations of the General Data Protection Regulation (GDPR), merchants are obliged to make data processing as transparent as possible for their customers with the information statutorily required by Articles 13 and 14 GDPR. This also applies to the processing of data in connection with payment transactions, and therefore also to the associated use of the 3DS 2.0 procedure. In the following, we would like to provide some information on the individual contents required by Articles 13 and 14 GDPR with regard to which merchants are obliged to provide information.

*- The following information shall only be a legally non-binding guideline for an essentially necessary case-related legal assessment and creatiion of a wording of the data protection information by the merchant and his data protection officer. –*

- **Identity and contact details of the controller and the controller's representative**

  *Note: Controller is the merchant.*

- **Contact details of the data protection officer**

  *Note: Data protection officer of the merchant*

- **Purposes for which personal data is intended to be processed and legal basis for the processing**

  *Note: To our opinion, generally the following purposes and legal bases can be considered. This information is not legally binding. Details should be assessed, specified and transferred into a wording on a case-related basis together with the merchant's data protection officer.*

**Legal implementation according to B. Alternative 1**

**Based on statutory permissions**

(The following purposes and legal bases must be legally assessed for all data elements individually):

**Purpose 1:** Performance of a contract. The end customer has entered into a contract with the merchant with a payment obligation and has consciously chosen a certain payment method at the check-out for the execution of which the transmission of certain data is required.
Legal basis: Article 6 section 1 sentence 1 lit. b GDPR.

**Purpose 2:** Performance of the strong customer authentication in accordance with the Directive EU 2015/2366 (PSD 2) resp. the Payment Services Supervision Act (PSA) (Zahlungsdiensteaufsichtsgesetz (ZAG).
Legal basis: Article 6 section 1 sentence 1 lit. c GDPR in conjunction with the corresponding provisions of the Directive EU 2015/2366 (PSD 2) resp. the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz - ZAG).

**Purpose 3:** Frictionless flow / optimization of conversion rates / user-friendliness (definition of "frictionless flow" see above).
Legal basis: Article 6 section 1 sentence 1 lit. f GDPR.
Legitimate interest according to Article 6 section 1 sentence 1 lit. f GDPR: Frictionless Flow / conversation optimization / user-friendliness

**Purpose 4:** Fraud prevention
Legal basis: Article 6 section 1 sentence 1 lit. f GDPR.
Legitimate interest according to Article 6 section 1 sentence 1 lit. f GDPR: In case of contracts that contain a credit risk resp. for which the contractual partner has a potential risk of non-payment, a legitimate interest can usually be assumed.

**Legal implementation according to B. Alternative 2**

**Incorporation into the contract**

(Within this alternative, purpose and legal basis apply to all data elements).

**Purpose:** Performance of a contract: Incorporation of corresponding information into the merchant's terms and conditions and legal justification with "necessity for the performance of a contract ".
Legal basis: Article 6 section 1, sentence 1 lit. b GDPR.

**Legal implementation according to B. Alternative 3**

**Obtaining of consents according data protection law**

(Within this alternative, purpose and legal basis apply to all data elements).

**Purpose:** Obtaining the buyer's consent at the check-out for performing an authentication resp. risk check.
Legal basis: Article 6 section 1 sentence 1 lit. a GDPR.

- **Categories of personal data concerned**

  *Note:* The individual data elements for the entire 3D Secure 2.0 procedure can be found in the latest version of the EMV specification (in the latest version of EMV specification 2.2.0 dated 18.12.2018, as linked in this document, see in particular Annex A 3-D Secure Data Elements, page 145 ff.).

- **Where the processing is based on Article 6(1)(f): Legitimate interests of the controller or a third party**

  *Note:* see above (listed under "Purposes for which personal data is intended to be processed and legal basis for the processing").

- **Recipients or categories of recipients of the personal data**

  *Note: Computop Wirtschaftsinformatik GmbH should be mentioned here as a processor according to Article 28 GDPR; Computop has been appointed with the technical steering of payment transactions, including the implementation of the 3D Secure 2.0 procedure. Further recipients are the banks involved (on the one hand the card-issuing bank - the issuer - and on the other the credit card-accepting bank of the merchant - the acquirer).*

- **Intention of the controller to transfer personal data to a third country or an international organisation (with information on the existence or absence of an adequacy decision by the Commission or, in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.**

  *Note: Data processing in the Computop Paygate, the payment platform of Computop Wirtschaftsinformatik GmbH, takes place in two data centers in Germany. Data may potentially be transferred to third countries in cases where the banks involved (on the one hand the card-issuing bank - the issuer - and on the other the credit card-accepting bank of the merchant - the acquirer) are based in third countries.*

- **Period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period**

  *Note: The Computop Paygate implements the following standardized deletion periods for payment transactions including 3DS 2.0 checks (unless a deletion has individually been requested beforehand):*

  - *Computop Paygate database and Computop Analytics: Deletion of payment transactions after 12 months.*
  - *Computop Reporter database: Deletion of payment transactions after 24 months.*
  - *Retention of database backups for the duration (and deletion of these backups after expiry) of further 12 months.*

  *The merchant is furthermore obliged to provide information about deletion periods in the merchant's*

*own systems (which might potentially be longer than within the Computop Paygate).*

- **Existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability**

  *Note: Here, the merchant can insert information that he uses as a standard for this point.*

- **Where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2): the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal**

  *Note: Only relevant if the merchant decides to obtain a consent at the check-out.*

- **Existence of a right to lodge a complaint with a supervisory authority**

  *Note: Here, the merchant can insert information that he uses as a standard for this point.*

- **Source from which the personal data originate and, if applicable, whether it came from publicly accessible sources**

  *Note: The data are originating from the contractual relationship with the merchant resp. from the customer account at the merchant or were generated as part of the transaction.*

- **Information about whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data**

  *Note:*

  *If the merchant decides to incorporate information relating to 3DS 2.0 and the data processed in this context into his merchant terms and conditions, he can thereby make the provision of personal data "a contractual requirement".*

  *A legal obligation to provide personal data may possibly be justified for some of the data elements by the fact that, in the context of the payment method that has been chosen, they are necessary for the performance of the legally required strong customer authentication according to the PSD2.*

  *Consequence of a failure to provide such data would be that the selected payment method cannot be executed.*

- **The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject**

  *Note: An automated authentication resp. risk check is being carried out. The effect might potentially be that the authentication might not be successful and that the selected payment method cannot be used in the specific case.*

---

*[1] Available at www.emvco.com; direct link to the latest version 2.2.0 of 18.12.2018: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo_3DS_SDKSpec_220_122018.pdf*
*[2] Also called: „2-factor-authentication", „Strong Customer Authentication" or „SCA".*
*[3] The term is defined in the EMV Spec.*
*[4] The term is defined in the EMV Spec.*
*[5] In the latest version of EMV Spec 2.2.0 dated 18.12.2018 – as linked in this document - see in particular Annex A 3-D Secure Data Elements, page 145 ff.*