HINWEISE AN AUFTRAGGEBER VON COMPUTOP IM SINNE DER DATENSCHUTZGRUNDVERODNUNG (DSGVO) ZU DATENSCHUTZRECHTLICHEN FRAGEN BEI DER NUTZUNG DES 3D-SECURE 2.0 VERFAHRENS

- Bitte beachten Sie, dass Zweck dieses Hinweisblattes lediglich ist, dem Händler als dem datenschutzrechtlichen Verantwortlichen und seinem Datenschutzbeauftragten eine Hilfestellung für eine zwingend erforderliche eigene einzelfallbezogene rechtliche Prüfung und Ausformulierung der datenschutzrechtlichen Informationen zu geben. Wir weisen zudem darauf hin, dass - obgleich der Inhalt dieses Hinweisblatts mit größter Sorgfalt recherchiert wurde - eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der Informationen nicht übernommen werden kann. -

A. ALLGEMEINES ZUM 3D-SECURE 2.0 VERFAHREN, ABLAUF

Das 3D-Secure 2.0 Verfahren (nachfolgend: 3DS 2.0) ist ein weltweit gültiger Standard der Kartennetzwerke (Visa, MasterCard, JCB, Diners, AMEX etc.), der durch die EMVCo, einen Verband der Kartennetzwerke, entwickelt wurde.

Einzelheiten zum 3DS 2.0 Verfahren können der jeweils aktuellsten Version der „EMV 3-D Secure Protocol and Core Functions Specification" (nachfolgend „EMV Spec", in der Fußnote verlinkt[1]) der EMVCo entnommen werden.

3DS 2.0 ist eines der Verfahren, mit der die starke Kundenauthentifizierung[2] nach der Richtlinie EU 2015/2366 (Payment Services Directive 2, PSD 2[3]) durchgeführt wird. Die PSD 2 ist in Deutschland im Zahlungsdiensteaufsichtsgesetz (ZAG) umgesetzt. Durch das 3DS 2.0 Verfahren wird bestätigt, dass die Person, die eine eCommerce Transaktion anstößt, auch berechtigt ist, die jeweilige Zahlungskarte zu nutzen.

Die Umstellung des 3DS Verfahrens von Version 1.0 auf Version 2.0 wirft derzeit verständlicherweise bei zahlreichen Händlern Fragen datenschutzrechtlicher Natur auf. Wir haben deshalb für Sie einige Informationen recherchiert und in diesem Hinweisblatt zusammengestellt. Hintergrund der allgemeinen Verunsicherung zu diesem Thema ist, dass Händler bei der Durchführung des neuen 3DS 2.0 Verfahrens potenziell bis zu 100 transaktions- und kundenbezogene Datenelemente mitsenden, die sich u.a. aus der Vertragsbeziehung des Händlers mit dem Käufer (z.B. Versandadresse oder Rechnungsadresse) oder aus dem Kundenkonto des Käufers beim Händler ergeben bzw. sich daraus ableiten lassen (z. B. Daten über die Konto-Nutzung durch den Käufer wie Bestehensdauer des Kontos oder Änderungshäufigkeit des Passwortes). Die entsprechenden Datenelemente werden im Rahmen des 3DS 2.0 Verfahrens an den Issuer, d.h. an die kartenausgebende Bank derjenigen Karte gesendet, mit der gezahlt werden soll.

Während das 3DS 1.0 Verfahren stets eine Interaktion des Käufers erforderte (wie z.B. eine Passwort- oder PIN-Eingabe) und deswegen mit sehr viel weniger Datenelementen auskam, wurden beim 3DS 2.0 Verfahren zahlreiche zusätzliche Datenelemente eingeführt, um einen sogenannten „Frictionless Flow"[4] zu ermöglichen, bei dem während des Authentifizierungsverfahrens keinerlei Interaktion des Karteninhabers erforderlich ist.

Das Authentifizierungsverfahren bei 3DS 2.0 sieht zwei Prüfungsebenen vor: Auf der ersten Prüfungsebene wird geprüft, ob aufgrund der durch den Händler mitgesendeten zusätzlichen Datenelemente ein „Frictionless Flow" möglich ist. Kommt das Authentifizierungsverfahren auf der ersten Prüfungsebene zum Ergebnis, dass ein „Frictionless Flow" nicht möglich ist, erfolgt auf der zweiten Prüfungsebene der sogenannte „Challenge Flow"[5], bei dem dann zusätzlich eine Interaktion des Karteninhabers erforderlich wird (Abfrage eines zweiten Faktors wie z.B. eine Passwort- oder PIN-Eingabe).

Sinn und Zweck des Frictionless Flow sind letztendlich die Erhöhung der Benutzerfreundlichkeit, die Steigerung von Konversionsraten und die Verhinderung von vorzeitigen Kaufabbrüchen. Je mehr Datenelemente ein Händler mitsendet, desto höher ist letztendlich die Wahrscheinlichkeit, dass ein Frictionless Flow möglich ist.

Die einzelnen Datenelemente für das gesamte 3DS 2.0 Verfahren können der jeweils aktuellsten Version der EMV Spec entnommen werden[6]. Manche dieser Datenelemente sind für die Durchführung des 3D-Secure 2.0 Verfahrens zwingend erforderlich, manche sind bedingt zwingend erforderlich (d.h. unter bestimmten Bedingungen zwingend erforderlich) und manche sind optional. Unter den bedingt zwingend erforderlichen Datenelementen finden sich in der EMV Spec auch solche, die mit dem Hinweis versehen sind „Required (if available) unless market or regional mandate restricts sending this information".

Bei den bedingt zwingend erforderlichen und den optionalen Datenelementen handelt es sich um solche, bei denen Händler prüfen müssen, ob es Gründe gibt (insb. rechtliche Gründe), aus denen die Datenelemente nicht mitgesendet werden können. Für die genannten Kategorien von Datenelementen ist eine Einzelfallprüfung des Händlers zusammen mit dessen Datenschutzbeauftragten notwendig.

B. REGELUNG DATENSCHUTZRECHTLICHER ASPEKTE IM ZUSAMMENHANG MIT DEM 3DS 2.0 VERFAHREN

Es gibt verschiedene Möglichkeiten, den Einsatz des 3DS 2.0 Verfahrens datenschutzrechtlich zu regeln:

Alternative 1:

Zugrundelegung gesetzlicher Erlaubnistatbestände

Für das Mitsenden der bis zu 100 transaktions- und kundenbezogenen Datenelementen können zunächst einige gesetzliche Erlaubnistatbestände geprüft werden.

Aus unserer Sicht kommen hier Artikel 6 Absatz 1 Satz 1 lit. b, c und f DSGVO in Betracht (Einzelheiten bzw. Hilfestellung zur Prüfung siehe unten C unter „Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung"). An dieser Stelle ist in jedem Fall für alle Datenelemente einzeln eine einzelfallbezogene Prüfung durch den Händler und seinen Datenschutzbeauftragten notwendig, die möglicherweise auch zu dem Ergebnis kommen kann, dass manche der Datenelemente nicht mitgesendet werden können.

Zur Erfüllung der datenschutzrechtlichen Informationspflicht nach Artikel 13, 14 DSGVO bei Zugrundelegung gesetzlicher Erlaubnistatbestände sollten die entsprechenden datenschutzrechtlichen Informationen (Einzelheiten siehe unten) möglichst direkt beim Check Out sowie in der Datenschutzerklärung der Webseite des Händler-Shops mit aufgenommen werden. Die Informationen beim Check Out können aus unserer Sicht auch zusammengefasst werden mit Verlinkung auf die Datenschutzerklärung, in der sich dann die vollständigen Informationen befinden. Je transparenter die Datenverarbeitung für den Kunden am Ende an dieser Stelle gemacht wird, desto besser!

Alternative 2:

Aufnahme in den Vertrag

Optional können Inhalte zu 3DS 2.0 zusammen mit allen datenschutzrechtlich erforderlichen Informationen nach Artikel 13, 14 DSGVO (siehe unten) auch in die Händler-AGB mit aufgenommen werden, die dem Vertrag mit dem Endkunden zugrunde liegen. Dies ist aus unserer Sicht zwar nicht zwingend erforderlich, hätte jedoch den Vorteil, dass Artikel 6 Absatz 1 Satz 1 lit. b DSGVO („Erforderlichkeit zur Vertragserfüllung") vermutlich durchgehend für alle Datenelemente als Rechtsgrundlage herangezogen werden könnte (im Sinne von Artikel 13 Absatz 2 lit. e DSGVO wäre dann die Bereitstellung der personenbezogenen Daten „vertraglich vorgeschrieben"). Sinnvoll ist die Wahl dieser Alternative insbesondere dann, wenn die rechtliche Einzelfallprüfung bei Alternative 1 ergeben haben sollte, dass Zweifel an der Zulässigkeit der Verarbeitung einzelner Datenelemente nach den gesetzlichen Erlaubnistatbeständen bestehen.

Zusätzlich empfehlen wir, die datenschutzrechtlichen Informationen nach Artikel 13, 14 DSGVO auch beim Check Out sowie in die Datenschutzerklärung des Händlershops mit aufzunehmen (beim Check Out ggf. zusammengefasst, siehe Hinweis bei Alternative 1).

Alternative 3:

Einholung einer datenschutzrechtlichen Einwilligungserklärung

Alternativ kann auch, sofern die rechtliche Prüfung im Rahmen von Alternative 1 ergeben sollte, dass Zweifel an der Zulässigkeit der Verarbeitung einzelner Datenelemente nach den gesetzlichen Erlaubnistatbeständen bestehen, überlegt werden, sicherheitshalber beim Check Out eine Einwilligungserklärung des Käufers gemäß Artikel 6 Absatz 1 Satz 1 lit. a DSGVO mit den datenschutzrechtlichen Informationen nach Artikel 13, 14 DSGVO einzuholen.

Zusätzlich sollten die Informationen nach Artikel 13, 14 DSGVO auch in die Datenschutzerklärung des Händlershops mit aufgenommen werden.

C. ERFÜLLUNG DER DATENSCHUTZRECHTLICHEN INFORMATIONSPFLICHT NACH ARTIKEL 13, 14 DSGVO

Nach den Vorschriften der EU Datenschutz Grundverordnung (DSGVO) sind Händler verpflichtet, Datenverarbeitungen für ihre Kunden mit den in Artikel 13 und 14 DSGVO gesetzlich vorgeschriebenen Informationen so transparent wie möglich zu machen. Dies gilt auch für Datenverarbeitungen im Zusammenhang mit Zahlungstransaktionen und daher auch für die damit einhergehende Nutzung des 3DS 2.0 Verfahrens. Nachfolgend möchten wir einige Hinweise zu den einzelnen nach Artikel 13 und 14 DSGVO vorgeschriebenen Inhalten geben, bezüglich derer Händler zur Information verpflichtet sind.

- Bei den nachfolgenden Hinweisen handelt es sich nur um eine rechtlich unverbindliche Hilfestellung für eine unbedingt notwendige einzelfallbezogene rechtliche Bewertung und Ausformulierung der datenschutzrechtlichen Informationen durch den Händler und seinen Datenschutzbeauftragten. –

- **Name und Kontaktdaten des Verantwortlichen und seines Vertreters**

  <u>Anmerkung</u>: Verantwortlicher ist der Händler

- **Kontaktdaten des Datenschutzbeauftragten**

  <u>Anmerkung</u>: Datenschutzbeauftragter des Händlers

- **Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung**

  Anmerkung: Aus unserer Sicht kommen allgemein folgende Zwecke und Rechtsgrundlagen in Betracht. Diese Hinweise sind rechtlich unverbindlich. Einzelheiten sollten einzelfallbezogen zusammen mit dem Datenschutzbeauftragten des Händlers bewertet, präzisiert und ausformuliert werden.

  Rechtliche Ausgestaltung gem. B. Alternative 1

  Zugrundelegung gesetzlicher Erlaubnistatbestände

  (Die nachfolgend genannten Zwecke und Rechtsgrundlagen müssen für alle Datenelemente einzeln rechtlich geprüft werden):

  Zweck 1: Vertragsdurchführung. Der Endkunde hat mit dem Händler zahlungspflichtig einen Vertrag abgeschlossen und hat beim Check Out bewusst eine bestimmte Zahlungsart gewählt, wobei für die Durchführung dieser Zahlung die Übermittlung bestimmter Daten erforderlich ist.
  Rechtsgrundlage: Artikel 6 Absatz 1 Satz 1 lit. b DSGVO.

  Zweck 2: Durchführung der starken Kundenauthentifizierung nach der Richtlinie EU 2015/2366 (PSD 2) bzw. dem Zahlungsdiensteaufsichtsgesetz (ZAG).
  Rechtsgrundlage: Artikel 6 Absatz 1 Satz 1 lit. c DSGVO i.V.m. mit den entsprechenden Regelungen der Richtlinie EU 2015/2366 (PSD 2) bzw. des Zahlungsdiensteaufsichtsgesetzes (ZAG).

  Zweck 3: Frictionless Flow / Optimierung von Konversionsraten / Benutzerfreundlichkeit (Definition von „Frictionless Flow" siehe oben).
  Rechtsgrundlage: Artikel 6 Absatz 1 Satz 1 lit. f DSGVO
  Berechtigtes Interesse im Rahmen von Artikel 6 Absatz 1 Satz 1 lit. f DSGVO: Frictionless Flow / Konversations-Optimierung / Benutzerfreundlichkeit

  Zweck 4: Betrugsprävention
  Rechtsgrundlage: Artikel 6 Absatz 1 Satz 1 lit. f DSGVO
  Berechtigtes Interesse im Rahmen von Artikel 6 Absatz 1 Satz 1 lit. f DSGVO: Bei Verträgen, die ein kreditorisches Risiko enthalten bzw. bei denen der Vertragspartner potenziell einen Zahlungsausfall befürchten muss, kann ein berechtigtes Interesse im Regelfall angenommen werden.

  Rechtliche Ausgestaltung gem. B. Alternative 2

  Aufnahme in den Vertrag

  (Zweck und Rechtsgrundlage gelten bei dieser Alternative für alle Datenelemente).

  Zweck: Vertragsdurchführung: Aufnahme entsprechender Informationen in die Händler-AGB und Begründung mit „Erforderlichkeit zur Vertragsdurchführung".
  Rechtsgrundlage: Artikel 6 Absatz 1 Satz 1 lit. b DSGVO.

  Rechtliche Ausgestaltung gem. B. Alternative 3

  Einholung einer datenschutzrechtlichen Einwilligungserklärung

  (Zweck und Rechtsgrundlage gelten bei dieser Alternative für alle Datenelemente).

  Zweck: Einholung einer Einwilligung des Käufers beim Check Out zur Durchführung einer Authentifizierung bzw. Risikoprüfung.
  Rechtsgrundlage: Artikel 6 Absatz 1 Satz 1 lit. a DSGVO.

- **Kategorien personenbezogener Daten, die verarbeitet werden**

  Anmerkung: Die einzelnen Datenelemente für das gesamte 3D Secure 2.0 Verfahren können der jeweils aktuellsten Version der EMV Spec entnommen werden (in der aktuellsten Version der EMV Spec 2.2.0 vom 18.12.2018, wie in diesem Dokument verlinkt, siehe insbesondere Annex A 3-D Secure Data Elements, Seite 145 ff.).

- **wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht: Berechtigte Interessen des Verantwortlichen oder eines Dritten**

  Anmerkung: siehe oben (im Rahmen der Zwecke und Rechtsgrundlagen aufgeführt).

- **Empfänger oder Kategorien von Empfängern der personenbezogenen Daten**

  Anmerkung: Hier ist zum einen die Computop Wirtschaftsinformatik GmbH als Auftragsverarbeiter nach Artikel 28 DSGVO zu nennen, der für die technische Steuerung von Zahlungstransaktionen einschließlich der Durchführung des 3D Secure 2.0 Verfahrens beauftragt wurde. Weitere Empfänger sind die involvierten Banken (zum einen die kartenausgebende Bank - der Issuer – und zum anderen die kreditkartenakzeptierende Bank des Händlers - der Acquirer).

- **Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln (mit Informationen über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind).**

  Anmerkung: Die Datenverarbeitung im Computop Paygate, der Zahlungsplattform der Computop Wirtschaftsinformatik GmbH, findet in zwei Rechenzentren in Deutschland statt. Zu einem Datentransfer in Drittländer kann es potenziell in Fällen kommen, in denen die involvierten Banken (zum einen die kartenausgebende Bank - der Issuer – und zum anderen die kreditkartenakzeptierende Bank des Händlers - der Acquirer) in Drittländern ansässig sind.

- **Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;**

  Anmerkung: Das Computop Paygate setzt standardmäßig folgende Löschfristen für Zahlungstransaktionen einschließlich 3DS 2.0 Prüfungen um (sofern nicht zuvor eine individuelle Löschung beauftragt wird):

  - *Computop Paygate Datenbank und Computop Analytics: Löschung von Zahlungstransaktionen nach Ablauf von 12 Monaten.*
  - *Computop Reporter Datenbank: Löschung von Zahlungstransaktionen nach Ablauf von 24 Monaten.*
  - *Aufbewahrung von Backups der Datenbanken für die Dauer (und Löschung dieser Backups nach Ablauf) von weiteren 12 Monaten.*

  Der Händler ist zudem verpflichtet, Informationen über Löschfristen in händler-eigenen Systemen zu geben (die ggf. länger sein können als im Computop Paygate)

- **Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;**

  Anmerkung: Hier können die durch den Händler standardmäßig zu diesem Punkt verwendeten Informationen eingefügt werden.

- **wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht: Das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird**

  Anmerkung: Nur relevant, sofern sich der Händler für eine Einwilligung beim Check Out entscheiden sollte.

- **Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde**

  Anmerkung: Hier können die durch den Händler standardmäßig zu diesem Punkt verwendeten Informationen eingefügt werden.

- **Quelle, aus der die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen**

  Anmerkung: Die Daten stammen aus der Vertragsbeziehung mit dem Händler bzw. aus dem Kundenkonto beim Händler oder wurden im Rahmen der Transaktion generiert.

- **Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte**

  Anmerkung:

  Sofern sich der Händler dafür entscheiden sollte, Inhalte zu 3DS 2.0 und den in diesem Zusammenhang verarbeiteten Daten in seine Händler-AGB mit aufzunehmen, kann er dadurch die Bereitstellung der personenbezogenen Daten „vertraglich vorschreiben".

  Eine gesetzliche Verpflichtung, die personenbezogenen Daten bereitzustellen, kann für manche der Datenelemente eventuell auch damit begründet werden, dass sie im Rahmen der gewählten Zahlungsmethode für die gesetzlich erforderliche starke Kundenauthentifizierung nach der PSD2 erforderlich sind.

  Folge der Nichtbereitstellung wäre, dass die gewählte Zahlungsart nicht durchgeführt werden kann.

- **Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.**

  Anmerkung: Es findet eine automatisierte Authentifizierungs- bzw. Risikoprüfung statt. Auswirkung kann potenziell sein, dass die Authentifizierung möglicherweise nicht erfolgreich ist und die gewählte Zahlungsart im konkreten Fall nicht genutzt werden kann.

---

[1] *Abrufbar unter www.emvco.com; direkter Link zur aktuellsten Version 2.2.0 vom 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] *Auch genannt: „2-Faktor-Authentifizierung", „Strong Customer Authentication" oder „SCA".*

[3][3] *Deutsch: Zweite Zahlungsdiensterichtlinie.*

[4] *Der Begriff ist in der EMV Spec definiert.*

[5] *Der Begriff ist in der EMV Spec definiert.*

[6] In der aktuellsten Version der EMV Spec 2.2.0 vom 18.12.2018 - wie in diesem Dokument verlinkt - siehe insbesondere Annex A 3-D Secure Data Elements, Seite 145 ff.