bankenverband

Verbraucherschutz im Zahlungsverkehr Übersicht und Ausblick

Innsbrucker Bankrechtsgespräche

Mag. Dr. Valeska Grond-Szucsich, LL.M.

Agenda

1. ZaDiG 2018
2. Verbraucherschutz im ZaDiG 2018
3. Spezialthemen:
    1. Änderungen des Rahmenvertrags
    2. Haftungsbestimmungen gem ZaDiG (inklusive Ausführung von Zahlungsaufträgen)
4. Dritte Zahlungsdienstleister
5. Ausblick auf PSD3, PSR und FIDA

Am 12.01.2016 ist die **zweite Zahlungsdiensterichtlinie** (EU) 2015/2366 („PSD2“) in Kraft getreten → war bis 13. Jänner 2018 in nationales Recht umzusetzen. PSD II ersetzt die **erste Zahlungsdiensterichtlinie** 2007/64/EG (ZaDiG alt).

Ziele der **maximalharmonisierten** PSD2:

- Weiterentwicklung des integrierten Binnenmarktes für Zahlungsdienste,
- weitere Stärkung des Verbraucherschutzes,
- Reduktion der mit Massenzahlungsverkehr verbundenen Risiken,
- Einbeziehung der technischen Innovationen bei den Zahlungsdiensten in den Regulierungsbereich.

01.06.2018: die PSD2 wird mit dem Zahlungsdienstegesetz 2018 (ZaDiG 2018) in Österreich umgesetzt. Damit trat das ZaDiG alt außer Kraft.

Einige Bestimmungen zur starken Kundenauthentifizierung und zur sicheren Kommunikation mit Drittdienstleistern ("Open Banking Schnittstelle") traten erst am **14.09.2019** in Kraft.

Die PSD2 wird ergänzt durch **Leitlinien** („GL“, „Guidelines“) und **Technische Regulierungsstandards** („RTS“, „Regulatory Technical Standards“) der Europäische Bankenaufsicht (EBA), mit denen die Anforderungen der Richtlinie präzisiert werden.

Aufbau des ZaDiG 2018

bankenverband

1. Hauptstück – Allgemeine Bestimmungen (§§ 1 - 6)

2. Hauptstück – Zahlungsdienstleister (§§ 7 - 31)

3. Hauptstück – Transparenz der Vertragsbedingungen und Informationspflichten für Zahlungsdienste

1. Abschnitt – Allgemeine Informationspflichten (§§ 32 - 38)
2. Abschnitt – Einzelzahlungen (§§ 39 - 45)
3. Abschnitt – Rahmenverträge (§§ 46 – 54)

bankenverband

4. Hauptstück – Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten (§§ 55 - 87)

1. Abschnitt – Gemeinsame Bestimmungen (§§ 55 - 57)
2. Abschnitt – Autorisierung von Zahlungsvorgängen (§§ 58 - 71)
3. Abschnitt – Ausführung von Zahlungsvorgängen (§§ 72 - 75)
4. Abschnitt – Ausführungsfrist und Wertstellungsdatum (§§ 76 - 78)
5. Abschnitt – Haftung (§§ 79 - 84)
6. Abschnitt – Operationelle und sicherheitsrelevante Risiken (§§ 85 - 87)

5. Hauptstück – Aufsicht, Strafbestimmungen und sonstige Maßnahmen (§§ 88 - 114)

6. Hauptstück – Übergangs- und Schlussbestimmungen (§§ 115 - 119)

Der Verbraucherbegriff des ZaDiG

Innsbrucker Bankrechtsgespräche
Verbraucherbegriff des ZaDiG

bankenverband

§ 4 Z 20 ZaDiG 2018:

*Verbraucher = eine **natürliche Person**, die bei den von diesem Bundesgesetz erfassten Zahlungsdienstverträgen zu Zwecken handelt, die nicht ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können*

- Die EK hat in ihren Q&As festgehalten, dass aufgrund des Vollharmonisierungsgebots nationale Definitionen des Verbrauchers im Anwendungsbereich der PSD nicht gelten **→ es gilt der engere europäische Verbraucherbegriff und nicht der des KSchG**.
- ZB Idealvereine, Privatstiftungen, Unternehmensgründer gelten nicht als Verbraucher iSd ZaDiG 2018.
- Was gilt für Gründungsgeschäfte?

Gründungsgeschäfte (vor Aufnahme des Betriebs von natürlichen Personen zur Schaffung der Voraussetzungen dafür getätigt) werden vom Geltungsbereich des KSchG umfasst. Im ZaDiG 2018 gibt es dafür keine Sonderregelungen → derartige Gründungsgeschäfte gelten iRd ZaDiG 2018 als unternehmensbezogene Geschäfte.

→ Personen (NP, JP), deren Zahlungsdiensteverträge einer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können, sind somit als Unternehmer zu qualifizieren.

§ 32 ZaDiG

§ 32 ZaDiG für das 3. Hauptstück (Transparenz der Vertragsbedingungen und Informationspflichten für Zahlungsdienste):

(1) Dieses Hauptstück gilt für Einzelzahlungen sowie für Rahmenverträge und die von ihnen erfassten Zahlungsvorgänge. Die Parteien können vereinbaren, dass dieses Hauptstück insgesamt oder teilweise nicht anzuwenden ist, wenn es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher handelt.

*(2) Soweit in Vereinbarungen **zum Nachteil eines Verbrauchers** von den Transparenz- und Informationspflichten dieses Hauptstücks **abgewichen** wird, sind diese abweichenden Bestimmungen **unwirksam**.* […]

§ 55 ZaDiG

bankenverband

§ 55 ZaDiG für das 4. Hauptstück (Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten):

(1) Handelt es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher, können der Zahlungsdienstnutzer und der Zahlungsdienstleister vereinbaren, dass § 56 Abs. 1, § 58 Abs. 3 sowie die §§ 66, 68, 70, 71, 74 und 80 ganz oder teilweise abbedungen werden. Der Zahlungsdienstnutzer und der Zahlungsdienstleister können auch andere als die in § 65 vorgesehenen Fristen vereinbaren (Rügeobliegenheit).

*(2) Soweit in Vereinbarungen **zum Nachteil eines Verbrauchers** von den Rechten und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten gemäß diesem Hauptstücks **abgewichen** wird, sind diese abweichenden Bestimmungen **unwirksam**. […]*

Innsbrucker Bankrechtsgespräche

Mit Unternehmern gem § 55 ZaDiG abdingbare Regelungen

ZaDiG	Regelung betreffend
§ 56 (1)	Entgeltvereinbarung (3 Nebenleistungen)
§ 58 (3)	Widerruflichkeit des Zahlungsauftrags bis zum Eintritt der Unwiderrufbarkeit
§ 65	Frist für Rügeobliegenheit vertraglich verkürzbar
§ 66	Nachweis der Authentifizierung und Ausführung von Zahlungsvorgängen
§ 68	Haftung des Zahlers für nicht autorisierte Zahlungsvorgänge
§ 70	Erstattung eines vom Zahlungsempfänger ausgelösten Zahlungsvorgangs
§ 71	Verfahren zur Erstattung eines vom Zahlungsempfänger ausgelösten Zahlungsvorgangs
§ 74	Unwiderruflichkeit von Zahlungsvorgängen
§ 80	Haftung des ZDL für nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen

Änderungen des Rahmenvertrags

- **§ 6 Abs 1 Z 2 KSchG**
  - Vertragsbestimmungen, nach denen
  - ein bestimmtes **Verhalten** des Verbrauchers **als Abgabe einer Erklärung gilt**
  - sind **nicht verbindlich**,
  - **es sei denn**,
  - der Verbraucher wird bei Beginn der hierfür vorgesehenen **Frist** auf die **Bedeutung** seines Verhaltens besonders **hingewiesen** und
  - hat **zur Abgabe einer ausdrücklichen Erklärung eine angemessene Frist**
- **ZaDiG**
  - § 50 Abs 1 iVm § 48 Abs 1 Z 6 lit a ZaDiG
  - § 29 Abs 1 iVm § 28 Abs 1 Z 6 lit a ZaDiG alt
- **Umsetzung der Zahlungsdiensterichtlinien** 2007/64/EG (PSD 1) bzw. 2015/2366/EU (PSD 2)
- **Vollharmonisierung**

Das ZaDiG sieht vor, dass eine Änderung des Rahmenvertrags mittels Zustimmfiktion wie folgt möglich ist:

- Der Zahlungsdienstleister (ZDL) und der Zahlungsdienstnutzer (ZDN) können **vereinbaren**, dass die **Zustimmung** des ZDN zu einer Änderung der Vertragsbedingungen **als erteilt gilt**, wenn er dem ZDL seine Ablehnung nicht vor dem geplanten Zeitpunkt des Inkrafttretens der Änderungen angezeigt hat.
- Der ZDL hat dem ZDN Änderungen des Rahmenvertrags spätestens **zwei Monate** vor dem geplanten Zeitpunkt ihrer Anwendung **vorzuschlagen** und **darauf hinzuweisen**, dass (i) die Zustimmung des ZDN als erteilt gilt, wenn er dem ZDL seine **Ablehnung** nicht vor dem vorgeschlagenen Zeitpunkt der Anwendung der Änderungen angezeigt hat, und (ii) dass der ZDN das **Recht** hat, den Rahmenvertrag vor dem Inkrafttreten der Änderungen **kostenlos fristlos zu kündigen**.

bankenverband

Vom OGH in der Leitentscheidung 1 Ob 210/12g formulierter „Grundsatz“ (RIS-Justiz RS0128865):

Eine Klausel, die Änderungen des Vertrags über eine Zustimmungsfiktion nach Inhalt und Ausmaß ***unbeschränkt*** *zulässt und* ***nicht einmal ansatzweise irgendeine Beschränkung erkennen lässt****, die den Verbraucher vor dem Eintritt unangemessener Nachteile schützen könnte, verstößt gegen das Transparenzgebot. Dies ist insbesondere dann der Fall, wenn die Klausel eine Änderung wesentlicher Pflichten der Parteien (Leistung und Gegenleistung) zugunsten des Verwenders der AGB* ***in nahezu jede Richtung und in unbeschränktem Ausmaß*** *zulässt. Es ist jedoch nicht jede Vertragsanpassung über eine in AGB vereinbarte Zustimmungsfiktion unzulässig, sondern nur eine* ***völlig uneingeschränkte****.*

bankenverband

Vom OGH in 1 Ob 210/12g für unwirksam erklärte Klausel:

Über die vorstehenden Abs 1 oder 2 hinausgehende Änderungen der Entgelte sowie Änderungen des Leistungsumfangs sind nur mit Zustimmung des Kunden möglich. Solche Änderungen werden 2 Monate nach Verständigung des Kunden über die vom Kreditinstitut gewünschte Änderung wirksam, sofern nicht bis dahin ein schriftlicher Widerspruch des Kunden beim Kreditinstitut einlangt. Das Kreditinstitut wird den Kunden in der Verständigung auf die jeweils gewünschte Änderung sowie darauf aufmerksam machen, dass sein Stillschweigen mit Fristablauf als Zustimmung gilt. Der Kunde hat das Recht, seinen Girokontovertrag bis zum Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Das Kreditinstitut wird den Kunden anlässlich der Mitteilung der Änderung auf dieses Kündigungsrecht aufmerksam machen.

bankenverband

Argumente des OGH für die Unzulässigkeit:

- Auch wenn die in der Klausel enthaltene Zustimmungsfiktion den **formalen Voraussetzungen** des § 6 Abs 1 Z 2 KSchG **entspricht**, ist **ihre Zulässigkeit** nach § 6 Abs 3 KSchG und § 879 Abs 3 ABGB **zu prüfen**.
- Die Klausel ist **intransparent**, weil sie Änderungen des Vertrags nach **Inhalt und Ausmaß** nahezu **unbeschränkt** zulässt. **Welche Leistungen** die Bank mit fingierter Zustimmung einschränken kann, bleibt völlig unbestimmt, ebenso der **Umfang einer Änderung** der vom Kunden zu entrichtenden **Entgelte**.
- Die Klausel ist **gröblich benachteiligend**, weil sie eine sehr weitgehende **Änderung von** (auch) **Hauptleistungspflichten** der Parteien bzw eine Änderung wesentlicher Pflichten (Leistung und Gegenleistung) zugunsten der Bank **in nahezu jede Richtung und im unbeschränkten Ausmaß** ermöglicht.

Vorabentscheidungsverfahren

Judikatur entwickelte sich in **ständige Rechtsprechung**

- **Kritik an dieser Judikatur:**
  - **§ 6 Abs 1 Z 2 KSchG** lässt Änderungen auch von Hauptleistungspflichten und Entgelten ausdrücklich zu. Eine im Verbotskatalog **ausdrücklich zugelassene Vereinbarung** kann nicht unwirksam sein.
  - **ZaDiG** lässt Änderungen des Rahmenvertrages (einschließlich der Hauptleistungen und Entgelte) ausdrücklich zu.
  - Mit **ZaDiG** wurde die **Zahlungsdiensterichtlinie** umgesetzt, der **vollharmonisierende Wirkung** zukommt. Der OGH hat das **Vollharmonisierungsgebot** der Richtlinie **missachtet** sowie seine **Vorlagepflicht an den EuGH verletzt** hat.
- Nachdem der OGH lange die Vorlage an den EuGh abgelehnt hatte, legt er im **Jänner 2019** folgende Frage zur **Vorabentscheidung** vor (OGH 25.01.2019, 8 Ob 24/18i)
  - Sind die Art 52 Z 6 iVm Art 54 Abs 1 PSD 2 dahin auszulegen, dass eine **Zustimmungsfiktion** auch mit einem Verbraucher „**völlig uneingeschränkt für sämtliche denkbaren Vertragsbedingungen" vereinbart** werden kann?

Innsbrucker Bankrechtsgespräche
8 Ob 105/20 d vom 25.03.2021

bankenverband

- **Antwort des EuGH C-287/19 (*DenizBank/VKI*) auf die Vorlagefrage:**
  - Art 52 Nr. 6 Buchst. A iVm Art 54 Abs 1 PSD II ist **dahin auszulegen**,
  - dass er die **Informationen und Vertragsbedingungen** bestimmt, die von einem Zahlungsdienstleister **mitzuteilen** sind, der mit dem Nutzer seiner Dienste gemäß den in diesen Bestimmungen vorgesehenen Modalitäten eine Vermutung der Zustimmung zur Änderung des Rahmenvertrags vereinbaren möchte,
  - dass er aber **keine Beschränkung** hinsichtlich der Eigenschaft des Nutzers oder der **Art der Vertragsbedingungen**, die Gegenstand einer solchen Vereinbarung sein können, festlegt
  - **hiervon unberührt bleibt jedoch**, wenn es sich bei dem Nutzer um einen Verbraucher handelt, die **Möglichkeit der Prüfung, ob diese Klausel** im Licht der Bestimmungen der RL 93/13/EWG über missbräuchliche Vertragsklauseln **missbräuchlich sind**

- **OGH-Urteil 8 Ob 105/20d vom 25.03.2021**

  - Mit der Antwort des EuGH C-287/19 *„wird klargestellt, dass die dargestellte ständige Rechtsprechung des Obersten Gerichtshofs mit den Vorgaben der Zahlungsdienste-Richtlinie vereinbar ist.“*

- **Entgeltänderung:**

Der Verbraucher muss von Anfang an aufgrund der Klausel **genau vorhersehen** können, **unter welchen konkreten Voraussetzungen**, die sachlich gerechtfertigt sein müssen, sich das Entgelt in welchem Ausmaß ändert bzw. eingeführt wird. Die Voraussetzungen müssen **eindeutig und transparent** sein; das Ausmaß möglicher Änderungen/Einführung muss beschränkt sein.

→ Indexanpassung.

- **Leistungsänderung:**

Auch für Änderungen von Leistungen gelten die Argumente der Judikatur zur Zustimmungsfiktion (1 Ob 210/12g). **Unzulässig sind daher Änderungsvorbehalte, die Änderungen nach Inhalt und Ausmaß nahezu unbeschränkt zulassen**. Insbesondere muss geregelt, **welche Leistungen** mit Zustimmungsfiktion geändert werden können. Die Leistungsänderung muss **sachlich gerechtfertigt** sein.

Die Haftungsbestimmungen des ZaDiG inklusive Ausführung von Zahlungsaufträgen

bankenverband

Typ 1: Haftung für **nicht autorisierte** Zahlungsvorgänge, §§ 67 ff

- 67: **Haftung des ZDL** für nicht autorisierte Zahlungsvorgänge
- 68: **Haftung des Zahlers** für nicht autorisierte Zahlungsvorgänge

- **Rügeobliegenheit** gem § 65
- **Nachweis Authentifizierung** durch ZDL gem § 66

- 70: Anspruch auf Erstattung eines **vom Zahlungsempfänger ausgelösten** Zahlungsvorgangs
- 71: **Verfahren** zur Erstattung eines vom Zahlungsempfänger ausgelösten Zahlungsvorgangs

Typ 2: Haftung für **nicht erfolgte/fehlerhafte** Ausführungen, §§ 79ff

- § 79: **Fehlerhafter Kundenidentifikator**
- § 80: **Haftung des ZDL** für die nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen
- § 81: **Haftung von Zahlungsauslösediensten** für die nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen
- § 82: Zusätzliche Entschädigung
- § 83: Regress
- § 84: Haftungsausschluss für ungewöhnliche und unvorhersehbare Ereignisse

- § 65 ZaDiG (Anzeige und Korrektur **nicht autorisierter oder fehlerhaft ausgeführter** Zahlungsvorgänge): Rügeobliegenheit (§ 65 ZaDiG) nach Feststellung des nicht autorisierten Zahlungsvorgangs; die **Frist**, um beim ZDL eine Berichtigung zu erwirken, endet spätestens **13 Monate nach dem Tag der Belastung** (sofern der ZDL seine gesetzlichen Informationspflichten erfüllt hat). Achtung: § 55 ZaDiG (ZDL und Unternehmerkunde können andere Frist vereinbaren).

- Verlust, Diebstahl, missbräuchliche Verwendung oder sonst nicht autorisierte Verwendung des Zahlungsinstruments (Karte) muss unverzüglich [sobald ZDN davon Kenntnis hat] angezeigt werden (§ 63 (2) ZaDiG).

Was bedeutet Authentifizierung?

bankenverband

§ 4 Z 27 ZaDiG

*Authentifizierung: ein **Verfahren**, mit dessen Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann;*

§ 4 Z 28 ZaDiG

*starke Kundenauthentifizierung: eine Authentifizierung unter Heranziehung von **mindestens zwei Elementen** der Kategorien **Wissen** (etwas, das nur der Nutzer weiß), **Besitz** (etwas, das nur der Nutzer besitzt) **oder Inhärenz** (etwas, das nur der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt* ist;

Haftungsfragen ZaDiG - § 66

bankenverband

ZDN **bestreitet Autorisierung** eines Zahlungsvorgangs **oder behauptet**, dass der Zahlungsvorgang **nicht ordnungsgemäß** ausgeführt wurde:

→ der ZDL muss nachweisen, dass

- der Zahlungsvorgang authentifiziert war,
- der Zahlungsvorgang ordnungsgemäß aufgezeichnet und verbucht wurde und
- nicht durch einen technischen Fehler oder eine andere Störung des vom ZDL erbrachten Dienstes beeinträchtigt wurde.

Wenn Zahlungsvorgang über Zahlungsauslösedienstleister ausgelöst → den TPP treffen innerhalb seines Zuständigkeitsbereiches diese Nachweispflichten.

Der bloße Nachweis der Nutzung eines Zahlungsinstruments reicht nicht aus als Nachweis

- der Autorisierung des Zahlungsvorgangs durch den Zahler,
- einer vorsätzlichen oder grob fahrlässigen Verletzung der Sorgfaltspflichten (§ 63) oder
- des Handelns des Zahlers in betrügerischer Absicht.

Jedenfalls muss der ZDL unterstützende Beweismittel vorlegen, um Betrug oder grobe Fahrlässigkeit des Zahlungsdienstnutzers nachzuweisen.

Typ 1
Haftung für nicht autorisierte Zahlungsvorgänge
§§ 67 ff

- **§ 67 ZaDiG: Haftung des ZDL für nicht autorisierte Zahlungsvorgänge**
- **§ 68 ZaDiG: Haftung des Zahlers für nicht autorisierte Zahlungsvorgänge**
- **§§ 65, 66, 69 – 71 ZaDiG**

bankenverband

Wann ist ein Zahlungsvorgang autorisiert (§ 58 ZaDiG)?

Ein Zahlungsvorgang gilt dann aus autorisiert, wenn der **Zahler** dem Zahlungsvorgang **zugestimmt** hat. Die Zustimmung erfolgt vor der Ausführung in der zwischen ZDN und ZDL vereinbarten Form und im vereinbarten Verfahren. Die Zustimmung kann über den Zahlungsempfänger oder einen Zahlungsauslösedienst erteilt werden.

Widerrufbarkeit bis zum Eintritt der Unwiderruflichkeit (§ 74 ZaDiG).

§ 67 ZaDiG normiert eine verschuldensunabhängige Haftung des ZDL für nicht autorisierte Zahlungsvorgänge:

Im Fall eines **nicht autorisierten Zahlungsvorgangs** hat der **ZDL** (unbeschadet des § 65 ZaDiG) **dem Zahler den Betrag** des nicht autorisierten Zahlungsvorgangs zu **erstatten**, außer wenn berechtigte Gründe einen Betrugsverdacht stützen.

Ausnahmen:

- § 57 ZaDiG: Kleinbetragszahlungen: ZDL und ZDN können vereinbaren, dass § 67 und § 68 (1-5) nicht anzuwenden sind.
- § 62 (1) Z 2 ZaDiG: Sperre des Zahlungsinstruments durch den ZDL beim Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines Zahlungsinstruments.

§ 68 ZaDiG regelt die Haftung des Zahlers für nicht autorisierte Zahlungsvorgänge:

Der Zahler haftet dem ZDL für nicht autorisierte Zahlungsvorgänge, die dem ZDL durch eine **missbräuchliche Verwendung des Zahlungsinstruments** entstehen, die der **Zahler** durch eine **schuldhafte Verletzung einer Pflicht gemäß § 63 ZaDiG** (zB Geheimhaltung von persönlichen Sicherheitsmerkmalen) **ermöglicht** hat.

Bei **leichter Fahrlässigkeit** ist die Haftung des Zahlers auf **max. EUR 50,--** beschränkt.

Hat der ZDL **keine starke Kundenauthentifizierung** verlangt, **haftet der Zahler nicht**, es sei denn, er hat in betrügerischer Absicht gehandelt.

Erstattung eines autorisierten Zahlungsvorgangs

Erstattung eines vom Zahlungsempfänger ausgelösten Zahlungsvorgangs (§ 70 ZaDiG) :

Zahler hat gegen ZDL **Anspruch auf Erstattung** eines autorisierten, vom oder über einen Empfänger ausgelösten Zahlungsvorgangs, wenn

- bei der Autorisierung der genaue Betrag nicht angegeben wurde und
- der Betrag des Zahlungsvorgangs den Betrag übersteigt, den der Zahler entsprechend seinem bisherigen Ausgabeverhalten, den Bedingungen seines Rahmenvertrags (Kartenvertrag) und den jeweiligen Umständen des Einzelfalles vernünftigerweise hätte erwarten können.

Auf Verlangen muss der Zahler dem ZDL die Sachumstände in Bezug auf diese Voraussetzungen darlegen.

Der Karteninhaber muss seinen Anspruch auf Erstattung binnen 8 Wochen ab Zeitpunkt der Belastung des Zahlungskontos mit dem betreffenden Geldbetrag geltend machen.

Typ 2
Haftung für nicht erfolgte/fehlerhafte Ausführungen
§§ 79 ff

- § 79 ZaDiG: Fehlerhafter Kundenidentifikator
- § 80 ZaDiG: Haftung des ZDL für die nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen
- § 81 ZaDiG: Haftung von Zahlungsauslösediensten für die nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen
- §§ 82 – 84 ZaDiG

bankenverband

Die Rolle des **Kundenidentifikators** (§ 79 ZaDiG):

- Zahlungsauftrag wird in Übereinstimmung mit dem **Kundenidentifikator** ausgeführt → gilt als korrekt ausgeführt (Pflicht zur **Kohärenzprüfung** durch ZDL).
- Wenn der vom ZDN angegebene Kundenidentifikator fehlerhaft ist → ZDL haftet nicht gem. § 80 für die nicht erfolgte oder fehlerhafte Ausführung des Zahlungsvorgangs → ABER: ZDL des Zahlers muss sich bemühen, Geldbetrag wiederzuerlangen. ZDL des Empfängers muss dem ZDL des Zahlers **alle maßgeblichen Informationen** erteilen.
- Der ZDL kann dem ZDN für die Wiedererlangung ein **Entgelt** verrechnen, wenn das im Rahmenvertrag vereinbart wurde.

bankenverband

§ 80: Haftung des ZDL bei nicht erfolgter oder fehlerhafter Ausführung von Zahlungsaufträgen (zB Fehlbuchungen, Malversationen, Systemversagen, etc.)

Wenn Zahler den Zahlungsauftrag direkt auslöst:

- ZDL des Zahlers haftet diesem gegenüber für die ordnungsgemäße Ausführung des Zahlungsvorgangs → er muss dem Zahler unverzüglich den Betrag des nicht oder fehlerhafte ausgeführten Zahlungsvorgangs erstatten und Konto valutagerecht richtigstellen

außer

- ZDL des Zahlers kann nachweisen, dass der Betrag des Zahlungsvorgangs fristgerecht beim ZDL des Empfängers eingelangt ist, dann haftet ZDL des Empfängers gegenüber dem Empfänger für die ordnungsgemäße Ausführung des Zahlungsvorgangs → er muss dem Empfänger unverzüglich den Betrag zur Verfügung stellen und dem Zahlungskonto des Empfängers gutschreiben (Korrekte Wertstellung gem § 78).

- Wenn der Zahlungsvorgang **verspätet ausgeführt** wird → ZDL des Empfängers muss auf Verlangen des ZDL des Zahlers sicherstellen, dass der Betrag auf dem Zahlungskonto des Empfängers korrekt wertgestellt wird (korrekte Wertstellung gem § 78).

- Auf Verlangen muss sich der ZDL des Zahlers unverzüglich bemühen, den Zahlungsvorgang zurückzuverfolgen und Zahler über Ergebnis informieren. Dafür darf ZDL kein Entgelt verlangen.

Wenn vom Zahlungsempfänger oder über diesen der Zahlungsauftrag ausgelöst wird:

- Der ZDL des Empfängers haftet diesem gegenüber für die ordnungsgemäße Übermittlung des Zahlungsauftrags an den ZDL des Zahlers (gem § 77 Abs 3). Wenn Ausführung nicht oder fehlerhaft erfolgt → unverzüglich nochmals Auftrag übermitteln.
- Verspätete Übermittlung → Betrag ist auf dem Zahlungskonto des Empfängers korrekt wertzustellen.
- Zudem haftet ZDL des Empfängers gegenüber dem Empfänger für die korrekte Bearbeitung des Zahlungsauftrags gem § 78 (Wertstellungsdatum). Der Betrag muss dem Empfänger unverzüglich zur Verfügung stehen, sobald er dem Zahlungskonto des ZDL des Empfängers gutgeschrieben wurde.

- Wenn ZDL des Zahlers nicht wie oben beschrieben haftet, haftet der ZDL des Zahlers gegenüber dem Zahler → er muss den Betrag erstatten und auf dem Konto des Zahlers valutagerecht wertstellen.
- Wenn der ZDL des Zahlers nachweist, dass der ZDL des Empfängers den Betrag mit einer geringfügigen Verzögerung erhalten hat → der Betrag ist vom ZDL des Empfängers auf dem Zahlungskonto des Empfängers valutagerecht wertzustellen.
- Der ZDL des Empfängers muss sich auf dessen Verlangen (ungeachtet der Haftungsregeln) unverzüglich darum zu bemühen, den Zahlungsvorgang zurückzuverfolgen. Der Zahlungsempfänger ist über das Ergebnis zu unterrichten. Dem Empfänger darf dafür kein Entgelt in Rechnung gestellt werden.

Darüber hinaus haften die ZDL gegenüber ihren jeweiligen ZDNn **für alle von ihnen zu verantwortenden Entgelte und Zinsen**, die dem Zahlungsdienstnutzer infolge der nicht erfolgten, fehlerhaften oder verspäteten Ausführung des Zahlungsvorgangs in Rechnung gestellt werden.

Haftung für nicht erfolgte oder fehlerhafte Ausführungen (§ 81)

- Wird ein Zahlungsauftrag vom Zahler über einen Zahlungsauslösedienstleister ausgelöst → der **kontoführende ZDL** muss dem Zahler den Betrag des nicht oder fehlerhaft ausgeführten Zahlungsvorgangs **erstatten** und das belastete Zahlungskonto valutagerecht **richtigstellen**.

- Der **Zahlungsauslösedienstleister hat nachzuweisen**, dass
  - der Zahlungsauftrag gemäß § 72 beim kontoführenden Zahlungsdienstleister des Zahlers eingegangen ist und
  - dass der Zahlungsvorgang innerhalb seines Zuständigkeitsbereichs authentifiziert, ordnungsgemäß aufgezeichnet und nicht durch ein technisches Versagen oder einen anderen Mangel im Zusammenhang mit der nicht erfolgten, fehlerhaften oder verspäteten Ausführung des Vorgangs beeinträchtigt wurde.

- **Regressmöglichkeit** des kontoführenden ZDL: haftet der Zahlungsauslösedienstleister für die nicht erfolgte, fehlerhafte oder verspätete Ausführung des Zahlungsvorgangs, so hat er dem kontoführenden Zahlungsdienstleister **auf dessen Verlangen** unverzüglich die infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge zu ersetzen.

- § 82: der Ersatz eines Schadens über die §§ 80 und 81 hinaus richtet sich nach den allgemeinen Bestimmungen.
- § 83: die Haftungsbestimmungen gem §§ 67 und 80 lassen Regressforderungen zwischen ZDLn oder zwischengeschalteten Stellen unberührt. Regressforderungen beinhalten zumindest alle gem den §§ 67 und 80 durch einen ZDL erlittenen Verluste oder gezahlten Beträge, auch Entschädigungen iZm Fällen, in denen der ZDL keine starke Kundenauthentifizierung verlangt.
- § 84: die Haftung gem §§ 58 bis 83 erstreckt sich **nicht auf ungewöhnliche und unvorhersehbare Ereignisse**, auf die diejenige Partei, die sich auf diese Ereignisse beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können, oder darauf, wenn ein ZDL durch gegenteilige unionsrechtliche, innerstaatliche, gerichtliche oder verwaltungsbehördliche Anordnungen gebunden ist.

Dritte Zahlungsdienstleister

Was kann bzw. darf wer und wie kommunizieren die Beteiligten?

bankenverband

Dritte Zahlungsdienstleiter = TPPs = „Third Party Provider"

- **Zahlungsauslösedienste:** § 1/2/7 ZaDiG = Dienste, die auf Antrag des ZDNs einen Zahlungsauftrag in Bezug auf ein bei einem anderen ZDL geführtes Zahlungskonto auslösen
- **Kontoinformationsdienste**: § 1/2/8 ZaDiG = Online-Dienste zur Mitteilung konsolidierter Informationen über ein oder mehrere Zahlungskonten, das/die ein ZDN bei einem anderen oder bei mehr als einem ZDL hält.
- § 59 ZaDiG: **ZDL, die kartengebundene Zahlungsinstrumente ausgeben** (und nicht der kontoführende ZDL sind)

Zahlungsauslösedienste und Kontoninformationdienste sind die von der PSD II neu definierten Zahlungsdienste.

Wenn sein **Konto online zugänglich** ist, hat der Zahlungsdienstnutzer das **Recht, einen TPP zu nutzen**.
Der kontoführende ZDL kann einem TPP nur dann den Zugang zu einem Zahlungskonto verweigern, wenn objektive und gebührend nachgewiesene Gründe iZm einem nicht autorisierten oder betrügerischen Zugang des TPP zum Zahlungskonto (inkl. nicht autorisierte oder betrügerische Auslösung eines Zahlungsvorgangs) dies rechtfertigen.

- diesbezügliche Informationspflicht gegenüber dem Zahler
- Zugangsverweigerung do lange, bis Gründe hierfür weggefallen
- Meldepflicht des kontoführenden Zahlungsdienstleisters gegenüber der zuständigen Behörde über Vorfall

TPPs: Pflichten des Zahlungsauslösedienstleisters

bankenverband

- Der Zahlungsauslösedienst darf zu keinem Zeitpunkt Geldbeträge des Zahlers halten.
- Die personalisierten Sicherheitsdaten des Zahlungsdienstnutzers dürfen nur dem Nutzer und dem Emittenten der personalisierten Sicherheitsdaten zugänglich sein.
- Die Informationen dürfen vom Zahlungsauslösedienst nur dem Zahler und dem Zahlungsempfänger nur mit ausdrücklicher Zustimmung des Zahlungsdienstnutzers mitgeteilt werden.
- Der TPP muss sich jedes Mal, wenn über ihn Zahlung ausgelöst wird, identifizieren und auf sichere Art kommunizieren.

TPPs: Pflichten des Zahlungsauslösedienstleisters

- Der TPP darf keine sensiblen Zahlungsdaten des Zahlungsdienstnutzers speichern. Der TPP darf die Daten nicht für andere Zwecke als für das Erbringen des vom Zahler ausdrücklich geforderten Zahlungsauslösedienstes verlangen, darauf zugreifen und speichern.
- Der Zahlungsauslösedienstleister darf vom Zahlungsdienstnutzer keine anderen als für das Erbringen des Zahlungsdienstes erforderlichen Daten verlangen.
- Der TPP darf den Betrag, den Empfänger oder ein anderes Merkmal des Zahlungsvorgangs nicht ändern.

Das Erbringen von Zahlungsauslösediensten darf nicht vom Bestehen eines Vertrags zwischen dem TPP und der kontoführenden Bank abhängig gemacht werden.

bankenverband

- Kommunikation mit dem Zahlungsauslösedienstleister auf sichere Weise
- Unmittelbar nach Eingang des Zahlungsauftrags von einem TPP sind diesem alle Informationen über die Auslösung des Zahlungsvorgangs und alle ihm selbst zugänglichen Informationen hinsichtlich der Ausführung des Zahlungsvorgangs mitzuteilen oder zugänglich zu machen.
- Behandlung der Aufträge ohne Diskriminierung

TPPs: Pflichten des Kontoinformationsdienstleisters

bankenverband

- Erbringung der Dienstleistungen nur mit ausdrücklicher Zustimmung des Zahlungsdienstnutzers.
- Die personalisierten Sicherheitsdaten des Zahlungsdienstnutzers dürfen nur dem Nutzer und dem Emittenten der personalisierten Sicherheitsdaten zugänglich sein.
- Der TPP muss sich jedes Mal, wenn über ihn Zugriff auf Konto erfolgt, identifizieren und sicher kommunizieren.
- Zugriff nur auf Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen.
- Keine Anforderung von sensiblen Zahlungsdaten, die mit den Zahlungskonten in Zusammenhang stehen.
- Daten dürfen nicht für andere Zwecke als für den vom Zahlungsdienstnutzer ausdrücklich geforderten Kontoinformationsdienst verwendet oder gespeichert werden bzw. auf diese zugegriffen werden.

bankenverband

- Kommunikation auf sichere Weise
- Datenanfragen von Kontoinformationsdienstleistern sind ohne Diskriminierung zu behandeln

Das Erbringen von Kontoinformationsdiensten darf nicht von einer vertraglichen Beziehung zwischen dem Kontoinformationsdienstleister und dem kontoführenden ZDL abhängig gemacht werden.

TPPs: ZDL, der kartengebundene Zahlungsinstrumente ausgibt und nicht gleichzeitig kontoführender ZDL („ASPSP“) ist

Unverzügliche Bestätigung durch ASPSP auf Ersuchen eines ZDL, der kartengebundene Zahlungsinstrumente ausgibt, ob ein Betrag, der für die Ausführung eines kartengebundenen Zahlungsvorgangs erforderlich ist, auf dem Zahlungskonto des Zahlers verfügbar ist, wenn:

- das Zahlungskonto des Zahlers ist zum Zeitpunkt des Ersuchens **online zugänglich**,
- der **Zahler hat dem ASPSP seine ausdrückliche Zustimmung** erteilt, den Ersuchen eines bestimmten ZDL um Bestätigung der Verfügbarkeit des Betrags, der einem bestimmten kartengebundenen Zahlungsvorgang entspricht, auf dem Zahlungskonto des Zahlers nachzukommen und
- die Zustimmung gemäß Z 2 ist erteilt worden, **bevor** das erste Ersuchen um Bestätigung ergeht.

TPPs: ZDL, der kartengebundene Zahlungsinstrumente ausgibt und nicht gleichzeitig kontoführender ZDL („ASPSP“) ist

Anfrage durch kartenausgebenden ZDL möglich, wenn

- der Zahler dem ZDL seine ausdrückliche Zustimmung erteilt, um die Bestätigung gemäß Abs. 1 zu ersuchen,
- der Zahler hat den kartengebundenen Zahlungsvorgang für den betreffenden Betrag unter Verwendung eines vom Zahlungsdienstleister ausgegebenen kartengebundenen Zahlungsinstruments ausgelöst und
- sich der ZDL gegenüber dem kontoführenden Zahlungsdienstleister vor jedem einzelnen Ersuchen um Bestätigung und kommuniziert mit dem kontoführenden Zahlungsdienstleister auf sichere Weiseauthentifiziert.

Die Bestätigung lautet nur auf „Ja“ oder „Nein“. Nicht erlaubt ist z.B. die Mitteilung des Kontostands. Die Antwort darf nicht gespeichert oder für andere Zwecke als für die Ausführung des kartengebundenen Zahlungsvorgangs verwendet werden.

Der ASPSP darf aufgrund der erteilten Bestätigung **keinen Geldbetrag** auf dem Zahlungskonto des Zahlers zu **blockieren**. Er muss dem Zahler auf Anfrage die Identifizierungsdaten des ZDL und die erteilte Antwort mitzuteilen.

Diese Bestimmung gilt **nicht** für Zahlungsvorgänge, die durch **kartengebundene Zahlungsinstrumente** ausgelöst wurden, auf denen **E-Geld** gemäß § 1 Abs. 1 des E- Geldgesetzes 2010 gespeichert ist.

Ausblick PSD3/PSR/FIDA

Am **12.01.2016** ist die **zweite Zahlungsdiensterichtlinie** (EU) 2015/2366 („PSD2“) in Kraft getreten → am **01.06.2018** in Österreich umgesetzt.

PSD2 ersetzte die **PSD1** [2007/64/EG (ZaDiG alt)]

Ziele der **maximalharmonisierten** PSD2:

- Weiterentwicklung des integrierten Binnenmarktes für Zahlungsdienste,
- weitere Stärkung des Verbraucherschutzes,
- Reduktion der mit Massenzahlungsverkehr verbundenen Risiken,
- Einbeziehung der technischen Innovationen bei den Zahlungsdiensten in den Regulierungsbereich

→ Und jetzt? **PSD3/PSR: laut EU-Kommission „Evolution, keine Revolution“**

(European Commission, Frequently Asked Questions zum Financial data access & payments package, 28.6.2023)

bankenverband

28.Juni 2023: Kommission veröffentlicht Regulierungsvorschlag:
Paket für den Zugang zu Finanzdaten und Zahlungen - Europäische Kommission (europa.eu)

Aus der PSD2 werden zwei Regularien:

- **PSR (Verordnung, direkt anwendbar): materielle Bestimmungen, zB**
  - vorvertraglichen Informationspflichten von Zahlungsdienstleistern,
  - Abschluss, Inhalt, Änderung und Beendigung von Zahlungsdiensteverträgen,
  - Erstattungsrechte / Haftungen,
  - Maßnahmen zur Betrugsbekämpfung,
  - Anforderungen im Zusammenhang mit der starken Kundenauthentifizierung (SCA)
- PSD3: Bestimmungen über Zulassungs- und Beaufsichtigung, EBA-Mandante für RTS, ITS und Leitlinien
- die E-Geld-Richtlinie wird wegfallen und in PSR/PSD3 integriert → E-Geldgeschäft wird Zahlungsdienst (kein „E-Geldinstitut“ mehr)
- Neu kommt dazu: Legislativvorschlag für einen Rahmen für den Zugang zu Finanzdaten (FIDA)

Absicht des Europäischen Gesetzgebers

Zahlungsverkehr und Finanzsektor sollen „**ins digitale Zeitalter**“ gebracht werden: Schwerpunkt liegt auf den Interessen, dem Wettbewerb, der Sicherheit und dem Vertrauen der Verbraucher.

- Verbesserung von Verbraucherschutz und Wettbewerb bei elektronischen Zahlungen
- Verbraucher sollen ihre Daten auf sichere Weise weitergeben können
- Verbrauchern soll dadurch ein breiteres Spektrum an besseren und billigeren Finanzprodukten und –dienstleistungen zur Verfügung stehen.

Elektronische Zahlungen in der EU sind stetig gewachsen:

2021: erreichten sie einen Wert von 240 Billionen EUR

Demgegenüber 2017: 184,2 Billionen EUR im Jahr 2017

Dieser Trend wurde durch die COVID-19-Pandemie beschleunigt.

EK Vorschläge zu Open Banking

EK hatte geprüft, Kontoinformationsdienstleister (AISPs) in der neuen Open-Finance-VO (FIDA) zu regulieren → bis dato nicht, aus heutiger Sicht geplant für den Zeitpunkt, wenn der Open-Finance-Rahmen voll funktionsfähig ist.

- PSR/PSD3-Vorschlag: bisherige PSD2-Standardregel bleibt: der kontoführende Zahlungsdienstleister (sg ASPSPs) muss Drittanbietern (Third Party Providers, TPPs) den Zugang zu Kontodaten ihrer Kunden ohne eine vertragliche Beziehung (und damit ohne Entgelt) ermöglichen müssen.
- Open Finance-Verordnung sieht jedoch für den Zugang zu anderen Finanzdaten - im Gegensatz zum PSR/PSD3-Vorschlag – die Möglichkeit vor, ein Entgelt zu verlangen.
- Neue Mindestanforderungen an die Leistungsfähigkeit der API-Schnittstellen festgelegt, va eine demonstrative Liste verbotener Übertragungshindernisse → das soll TPPs einen optimalen Datenzugang zum vollen Nutzen ihrer Kunden gewährleisten.

EK Vorschläge zu Open Banking

- Die derzeitige Anforderung, TPPs einen "Fallback Mechanism" (Notfallmechanismus) zur Verfügung zu stellen, wird gestrichen (nur mehr Pflicht zur Aufrechterhaltung einer dedizierte Schnittstelle). Weiters müssen TPPs die Möglichkeit haben, bei einem Ausfall der Schnittstelle die Geschäftskontinuität durch einen vorübergehenden Notfalldatenzugriff aufrechtzuerhalten.
- ASPSPs sollen weiters verpflichtet werden, ihren Kunden ein sg "Permission Dashboard" anzubieten. Dieses soll es Kontoinhabern ermöglichen, auf einen Blick im Zahlungskonto zu sehen, wem sie welche Datenzugriffsrechte gewährt haben. Kunden sollen zudem die Möglichkeit haben, über dieses Tool Datenzugriffe Dritter zu beenden, wenn sie dies wünschen.

Katalog der Zahlungsdienste / Anwendungsbereich

bankenverband

EK will den Anwendungsbereich der PSD2 laut eigenen Angaben nicht verändern:

Der Katalog der konzessionspflichtigen Zahlungsdienste bleibt weitgehend unverändert, abgesehen von einigen Anpassungen:

- Ein- und Auszahlungsgeschäft werden in einem Tatbestand zusammengefasst
- „Führung von Zahlungskonten“ entfällt
- Zahlungsgeschäft ohne und mit Kreditgewährung wird in einem Tatbestand geregelt werden
- Issuing und Acquiring werden als getrennte Zahlungsdienste definiert (offen ist, ob Acquirer und Issuer künftig noch Kredite anbieten dürfen.
- Neue Definition für E-Geldgeschäft (in Annex 2 zur PSR)
  - Ausgabe von E-Geld (= bisherige Definition in der 2. E-Geld-Richtlinie)
  - Führung von Zahlungskonten, auf denen E-Geld gespeichert ist
  - Transfer von E-Geldeinheiten

Betrugsbekämpfung

Betrugsbekämpfung im Zahlungsverkehr = **sehr wichtiges Anliegen der EK**, insbesondere wegen der Entwicklung neuer Betrugsarten in den letzten Jahren, zB "Social-Engineering-Betrug“.

- **Kampf gegen "Spoofing“**: Problem = Unterscheidung zwischen autorisierten und nicht autorisierten Transaktionen verschwimmt, da die vom Kunden erteilte Zustimmung zur Autorisierung einer Transaktion von Betrügern manipuliert wird, indem sie zB die Telefonnummer oder E-Mail-Adresse der Bank verwenden.

Vorgeschlagene Bekämpfungsmaßnahmen:

- **IBAN/Namens-Prüfung (sg "IBAN-name check")**: bei allen Überweisungen in EU-Währungen = dre Zahlungsdienstleister des Zahlungsempfängers wird verpflichtet, bei Überweisungen in einer EU-Währung unentgeltlich die Übereinstimmung des IBANs des Zahlungsempfängers mit dem Kontonamen zu prüfen und dies dem ZDL des Auftraggebers mitzuteilen. Einen derartige Verpflichtung gibt es bis dato in der Verordnung für Instant Payments.

bankenverband

Weitere vorgeschlagene Bekämpfungsmaßnahmen:

- eine **stärkere Transaktionsüberwachung**, um eine starke Kundenauthentifizierung zu gewährleisten und die Prävention und Aufdeckung betrügerischer Transaktionen zu verbessern. In diesem Zusammenhang ist die Schaffung einer DSGVO-konformen Regelung geplant, damit die Zahlungsdienstleister betrugsbezogene Informationen untereinander austauschen können;
- eine Verpflichtung der Zahlungsdienstleister zur **Durchführung von Aufklärungsmaßnahmen**, um ihre Kunden und Mitarbeiter für Betrug im Zahlungsverkehr zu sensibilisieren; und
- eine **Ausweitung der Erstattungsrechte der Verbraucher** in bestimmten Situationen

Erweiterung der Haftung der PSP

Vorschlag beinhaltet eine Erweiterung der Haftungsregeln zulasten von Zahlungsdienstleistern:

Geplant ist die Gewährung von Erstattungsansprüchen:

- für Verbraucher, die einen Schaden erlitten haben, weil der **"IBAN-name check"** eine Abweichung zwischen dem Namen und der IBAN des Zahlungsempfängers nicht erkannt hat, und
- für Verbraucher, die Opfer eines **"Spoofing"-Betrugs** geworden sind. Hier kontaktiert der Betrüger den Verbraucher unter dem Vorwand, ein Angestellter der Bank des Verbrauchers zu sein. Er bringt den Verbraucher dazu, bestimmte Handlungen vorzunehmen, die dem Verbraucher einen finanziellen Schaden verursachen.

bankenverband

Was bedeutet das?

- Das bedeutet, dass Opfer von Spoofing-Betrug von ihrer kontoführenden Bank die Erstattung des vollen Betrags der betrügerischen Transaktion verlangen dürfen, wenn sie eine polizeiliche Anzeige über den Spoofing-Betrug erstatten und ihre Bank unverzüglich darüber informieren.
- Das "Spoofing" muss überzeugend sein, zB durch die exakte Nachbildung der E-Mail-Adresse oder Telefonnummer der Bank.
- Ausnahme: Dann keine Erstattung, wenn der Verbraucher grob fahrlässig (zB wenn er mehrfach auf denselben Betrug hereinfällt) oder in Betrugsabsicht gehandelt hat. Die **Beweislast** für ein grob fahrlässiges bzw betrügerisches Handeln des Verbrauchers liegt jedoch beim **Zahlungsdienstleister**.

Dieser Vorschlag führt zu Haftungen in Situationen, gegen die eine Bank nichts dagegen unternehmen kann!

bankenverband

Die starke Kundenauthentifizierung (SCA) = 2-Faktor-Authentifizierung = eine zentrale Maßnahme der PSD2 zur Verhinderung von Betrug:

Zahlungsdienstnutzer identifizieren sich durch mindestens zwei Elemente aus den Kategorien Wissen (zB ein PIN), Besitz (zB eine Zahlungskarte) und Inhärenz (zB ein Fingerabdruck).

Näheres zur SCA ist in RTS geregelt:

Delegierte Verordnung über technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation)

Der PSR-Vorschlag enthält Details zu Neuerungen bei den SCA-Vorgaben.

bankenverband

- Es sollen künftig **barrierefreie SCA-Tools** bereitgestellt werden, die speziell von Menschen mit Behinderungen, älteren Menschen sowie anderen Personen, die Schwierigkeiten bei der Nutzung von SCA haben, verwendet werden können, zB soll ein Smartphone keine Voraussetzung sein, um sich zu authentifizieren.
  - (Siehe RL zur Barrierefreiheit: Richtlinie über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen).

- **MIT**s = von Händlern ausgelöste Zahlungsvorgängen = "merchant-initiated transactions“: es soll keine SCA erforderlich sein, wenn ein Zahlungsvorgang ohne jegliche Beteiligung des Zahlers ausgelöst wird. Wenn ein MIT aufgrund eines Mandats des Zahlers erfolgt, ist eine SCA nur bei der Einrichtung des Mandats notwendig, bei nachfolgenden Zahlungsvorgängen nicht.

- **MOTO**s = telefonische oder Mail-Order-Bestellungen: eine nicht digitale Auslösung des Zahlungsvorgangs soll unter der Voraussetzung, dass der Zahlungsdienstleister des Zahlers Sicherheitsanforderungen und -kontrollen durchführt, die eine Form der Authentifizierung des Zahlungsvorgangs ermöglichen, keiner Verpflichtung zur SCA unterliegen.

- Gem PSD2 müssen ASPSPs mindestens **alle 90 Tage** eine **starke Kundenauthentifizierung** ihrer Nutzer durchführen, die über einen bestimmten Kontoinformationsdienstleister (AISPs) auf ihr Zahlungskonto zugreifen. Die PSR sieht vor, dass ASPSPs bei der **erstmaligen Anwendung** und dann nur mehr **alle 180 Tage** eine SCA durchführen müssen. Außerdem sollen AISPs die Möglichkeit erhalten, selbst eine SCA durchzuführen.

bankenverband

Zur Verbesserung des Verbraucherschutzes schlägt die EK weitere Maßnahmen vor, zB

- Das **Surcharging-Verbot** soll auf alle Überweisungen und Lastschriften in allen Währungen ausgeweitet werden.
- Betreffend Überweisungen und Geldtransfers aus der EU in Drittländer:
  - Nutzer sollen entsprechend den derzeitigen Informationspflichten für Transaktionen innerhalb der EU über die voraussichtlichen Gebühren für die Währungsumrechnung informiert werden müssen.
  - Kunden sollen über die voraussichtliche Dauer bis zum Eingang des Betrags beim Zahlungsdienstleister des Zahlungsempfängers in einem Drittland informiert werden. Es wird jedoch keine Maximalfrist für derartige Überweisungen und Geldtransfers verlangt – eine solche wäre nicht realisierbar, da die Dauer teilweise von Banken außerhalb der EU abhängt, die auch nicht den EU-Vorschriften unterliegen.

Einstufung digitaler Wallets

Im Vorfeld wurde diskutiert, ob bestimmte digitale Wallet-Anbieter bzw andere technische Dienstleister im Rahmen der PSD3 reguliert werden sollen.

- Im PSR/PSD3-Vorschlag der EK ist vorgesehen, dass sog "pass-through wallets", wie etwa Apple Pay und Google Pay, kein Zahlungsinstrument darstellen, sondern einen **technischen Dienst**.
- Vorschlag sieht Abschluss eines **Outsourcing-Vertrags** von Anbietern solcher Wallets mit dem Issuer des jeweiligen Zahlungsinstruments vor, wenn Transaktionen mit Hilfe von Elementen der SCA autorisiert werden sollen, zB mit dem Emittenten der Kreditkarte, die in der Wallet tokenisiert wird.
- Andere Kategorien digitaler Geldbörsen hingegen, zB vorausbezahlte elektronische Geldbörsen wie "staged wallets", in denen die Nutzer Geld für künftige Online-Transaktionen speichern können, sollen jedoch als Zahlungsinstrument und ihre Ausgabe als Zahlungsdienst betrachtet werden.
- NFC ist per se kein Zahlungsinstrument.

Mögliche Timeline PSD3/PSR

- 28.6.2023: Vorschläge der Kommission
- Positionen von Rat (Juni 2024?) und Parlament (April 2024)

  - EP: Bericht veröffentlicht

  PR_COD_1consamCom (europa.eu)

  - Rat: große Diskussionsthemen: Autorisierung, grobe Fahrlässigkeit, Betrugsprävention
- Trilog-Verhandlungen ab Herbst 2024 bis Anfang/Mitte 2025?
- In-Kraft-Treten Mitte/Ende 2025?
- 18 Monate Umsetzungsfrist
- Anwendbar ab Ende 2026/2027?

Vielen Dank für Ihr Interesse!

Mag. Dr. Valeska Grond-Szucsich, LL.M.

Verband österreichischer Banken & Bankiers
A-1010 Wien, Börsegasse 11
Telefon: +43 1 535 17 71 - 26
grond@bankenverband.at