SPIRIT LEGAL®

MaSI

Das BaFin-Rundschreiben zu Mindestanforderungen im Zahlungsverkehr

OTMR 2015, Leipzig

Wer wir sind, was wir machen

Spezialisierung, Branchen & Netzwerk

Spirit Legal LLP Rechtsanwälte

- *Sozietät für IT- und Wirtschaftsrecht*

Themen & Branchen:

- *Handel mit Waren & Dienstleistungen*
- *Vertrieb*
- *Marketing*
- *Tourismuswirtschaft*

Spezialisierung

- *IT & Datenschutzrecht*
- *Onlinevertriebsrecht & Payment*
- *Wettbewerbsrecht*
- *Marken & Domains*

Zahlungsrisiken im SEPA-Raum

EZB Statistik 2012:

- 1€ Missbrauch aus 2.635 € Karten (Kredit/Debit)-Umsatz
- 0,038 % des Gesamttransaktionsvolumens von 2,5 Trillionen EUR Kartenzahlungen
- Gesamtwert missbräuchlicher Transkationen: 1,33 Mrd. EUR

Regulierungsbehörden

wer spielt hier mit?

EUROPÄISCHE ZENTRALBANK

EUROSYSTEM

EBA European Banking Authority

European System of Financial Supervision

BaFin

Regulierungsversuche

Wann?	Was?
2011	Erster Entwurf der EZB SecuRe Pay Recommendations
Januar 2013	Finaler Entwurf EZB SecuRe Pay Empfehhlungen für die Sicherheit von mobilen Zahlungen
Mai 2014	Final ECB SecurRe Pay Recommendation on the security of account access services
Herbst 2014	Vereinbarung EZB/EBA über Veröffentlichung Sicherheitsrichtlinien für Internetzahlungen durch EBA
Oktober 2014	Öffentliche Anhörung der EBA zu dem Entwurf der EBA Leitlinien (identisch mit ECB SecuRe Pay)
19. Dezember 2014	Final EBA Guidelines / LL „Leitlinien zur Sicherheit von Internetzahlungen“
Februar 2015	**BaFin - Konsultation zum Entwurf des MaSi-Rundschreibens**
5. Mai 2015	**BaFin - Veröffentlichung MaSi-Rundschreiben**
5. November 2015	**Ende Umsetzungsfrist (Nichtanwendungsversprechen)**
2017	Umsetzung PSDII

Umsetzung EBA-LL in 28 Mitgliedstaaten

Comply or Explain bis Mai 2015!

- UK: Anfang/Mitte 2017, mit Umsetzung PSDII
- Bulgarien, Liechtenstein, Ungarn: noch offen
- Deutschland, Frankreich, Finnland, Österreich:

  verspätet, nach August 2015
- Italien seit 01.02.2015
- alle anderen MGS: 01.08.2015

MaSi – Rundschreiben vom 05.05.2015

Wenn der Postmann zweimal klingelt…

BaFin

Bundesanstalt für Finanzdienstleistungsaufsicht

English | Kontakt | RSS | Newsletter | Gebärdensprache | Leichte Sprache

Suchbegriff

Aufsicht | Verbraucher | Internationales | Die BaFin | Daten & Dokumente

Inhalt

- Alle Dokumente
- Alle Datenbanken
- Aufgehobene Dokumente
- BaFinJournal
- MVP Portal

Startseite ▸ Daten & Dokumente ▸ Rundschreiben ▸ Rundschreiben 4/2015 (BA) - Mindestanforderungen an die Sicherheit von Internetzahlungen

Rundschreiben 4/2015 (BA) - Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)

Geschäftszeichen BA 57-K 3142-2013/0017

Bonn/Frankfurt a. M., 5. Mai 2015

An alle Zahlungsdienstleister in der Bundesrepublik Deutschland

MaSi – Hehre Ziele…

„(…)
Ziel ist es,
ganzheitlichen Schutz
vor Cyber-Kriminalität
zu gewährleisten.
(…)“

MaSi – …und was daraus wurde

- reine <u>Übersetzung</u> der EBA-Leitlinien
- Vorsicht geboten bei Auslegung:

EBA-LL sagt…	BaFin sagt…	BaFin meint…
should	sollten	müssen!

- <u>Mindesterwartungen:</u>

  Ergebnisse <u>ohne</u> Lösungswege
  Umsetzungsrisiko trägt PSP

MaSi – Inhalt

Titel I	Anwendungsbereich und Begriffsbestimmungen
Titel II	Rundschreiben zu den Mindestanforderungen an die Sicherheit von Internetzahlungen
	Allgemeines Kontroll- und Sicherheitsumfeld
	Spezifische Kontroll- und Sicherheitsmaßnahmen für Internetzahlungen
	Kundenaufklärung, -information und -kommunikation
Anhang 1:	Beispiele für bewährte Vorgehensweisen (bV)
	Allgemeines Kontroll- und Sicherheitsumfeld
	Spezifische Kontroll- und Sicherheitsmaßnahmen für Internetzahlungen

MaSI – Rechtliche Auswirkungen

Welche Folgen hat das neue Rundschreiben?

- Stärker ausgeglichene Regulierungsstandards zwischen Kreditinstituten und ZDK bei Erbringung derselben DL > Reduzierung des Wettbewerbsvorteils für Nicht-Banken

- Erheblicher Anpassungsbedarf bei Verträgen zwischen PSP und Online-Händlern über Abrechnungsdienste & Outsourcingdiensten , wenn Sicherheit der Internetzahlungsdienste betroffen ist

- Implementierung neuer Risikomanagement-Prozesse beim PSP

MaSI – Wirtschaftliche Auswirkungen

Welche Folgen hat das neue Rundschreiben?

- Marktverschiebungen zu bestimmten Zahlungsarten
  - durch zusätzliche Prozessschritte führen
  - Belastung Transaktionskosten

- E-Händler könnten ausländische ZDL bevorzugen

- Einfluss auf Conversion-Rate

MaSI – Persönlicher Anwendungsbereich

Adressaten der Regelungen

Erfasst

- Kreditinstitute, Zahlungsinstitute
- E-Geld-Institute
- Mittelbar: Nutzer der Zahlungmethoden (E-Händler)

Nicht erfasst

- „Dritte Zahlungsdienstleister“
- Zahlungsauslösedienste/Kontoinformationsdienst
- Technische Dienstleister für PSP

MaSI – Sachlicher Anwendungsbereich

Was ist umfasst?

- Internetzahlungsdienste wenn browserbasiert
- Karten, auch virtuelle Kartenzahlungen elektronische Geldbörsen (E-Wallet)
- Überweisungen
- Elektronische Einzugsermächtigung/Lastschrift
- E-Geld

MaSI – Sachlicher Anwendungsbereich

*Was ist **nicht** umfasst?*

- Online-Brokerage, Online-Verträge
- Zahlungen per Post/Telefon/Voicemail/SMS
- mobile Zahlungen (App), aber Rückausnahme: browserbasierten Zahlungen
- Überweisungen, bei denen ein Dritter auf das Zahlungskonto des Kunden zugreift
- Zahlungsvorgänge innerhalb eines unternehmensinternen Netzwerks
- Kartenzahlungen mit anonymen/nicht aufladbarer/virtueller Karten auf Guthabenbasis
- Clearing und Verrechnung von Zahlungsvorgängen

MaSI – Authentifierung vs. Starke Authentifizierung

- Wann:
  - bei Auslösung von Zahlungen
  - bei Zugriff aus sensible Zahlungsdaten

- Authentifizierung:
  - Verfahren, das dem PSD die Überprüfung der Identität eines Kunden ermöglicht (wie bei GWG)

- Starke Authentifizierung:
  - *qualifiziertes* Verfahren, Authentifizierung unter Verwendung besonderer Elemente

MaSI – Verfahren der Authentifizierung

- Vertraulichkeit der Authentifizierungsdaten gewährleisten
- Daten dürfen nicht heimlich über das Internet entwendet werden können
- Sicherheit des Authentifizerungsverfahrens muss zertifiziert sein (z. B. vom BSI), Prüfung ist laufend zu wiederholen

MaSI – Erstidentifikation des Kunden & Information

- in Einklang mit GWG

- Information durch PSP in angemessener Weise regelmäßig, vorab und ggf. kurzfristig über Voraussetzungen für die Durchführung sicherer Internetzahlungsvorgänge

- Vorschlag BaFin als „bewährte Vorgehensweise“: Faltblatt

MaSI – Erstidentifikation des Kunden

- Vorlage geeigneter Ausweisdokumente und damit verbundener Informationen

- bevor Zugang zu den Internetzahlungsdiensten gewährt wird

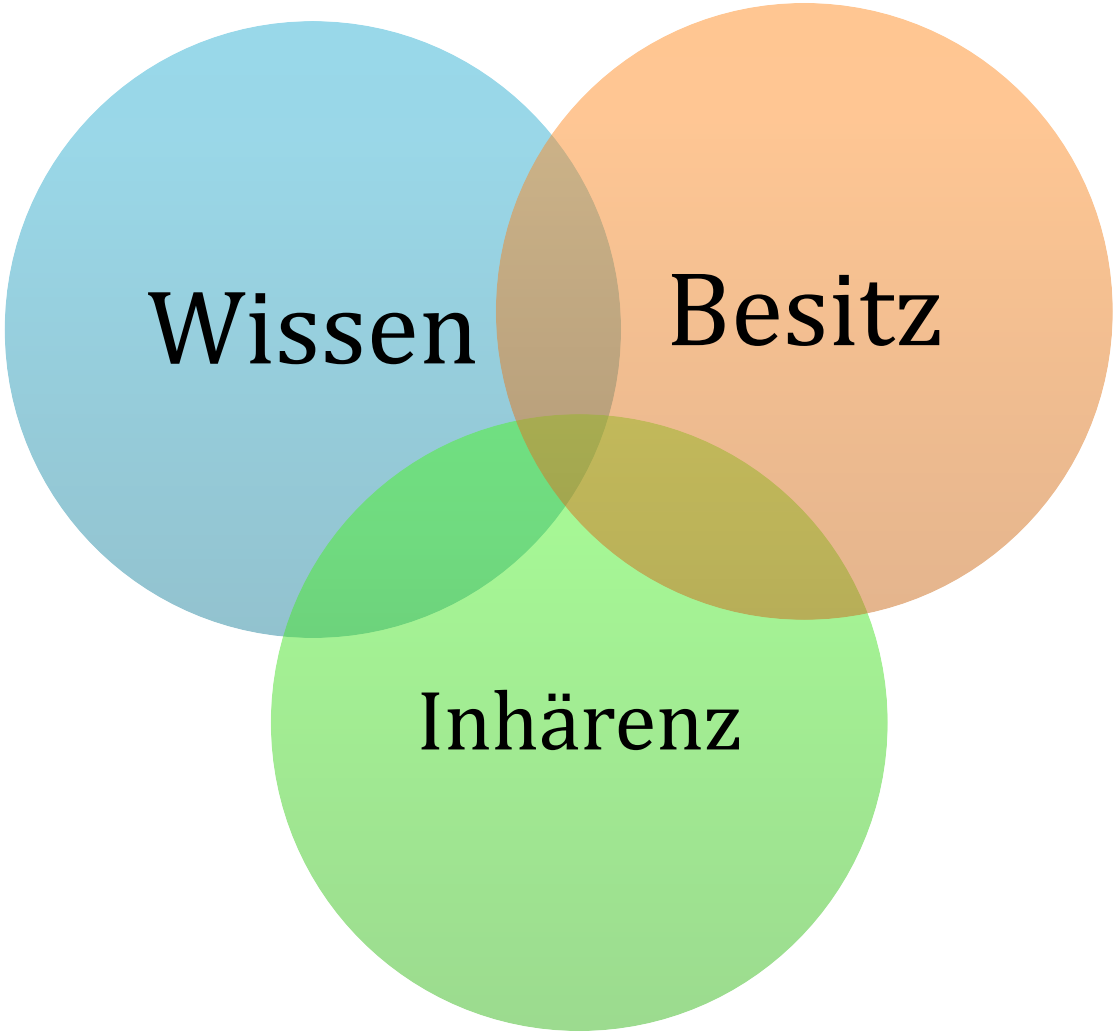
Beispiele:
Number26, Ing Diba, Commerzbank > Idnow GmbH

MaSI – Wann ist die Str. Auth. erfoderlich?

1. **Auslösung von Internetzahlungen**
2. Zugang zu sensiblen Zahlungsdaten
3. Elektronische Geldbörsen
4. Ausgabe virtueller Karten
5. Kommunikation zwischen ZDL und E-Händlern

MaSI – Starke Kundenauthentifizierung

Die Elemente



MaSI – Element Wissen

Ja	Nein
• Statisches Passwort • Code • PIN (zB 3-D Secure / Verified by Visa)	• Kontonummer* • Kreditkartennummer* • Geburtsdatum* • CVC-Nummer** • TAN**

MaSI – Element Besitz

Ja	Nein
• beim ZDL registrierte Kennung des Nutzers* • CVC-Nummer • Token • Smartcard • Mobiltelefon	• Kontonummer • Kreditkartennummer

MaSI – Element Inhärenz

Ja	Nein

• Fingerabdrücke
• Iris-Scan
• Gesicht, Körper
• Stimme, Gangart (Erfassen über Smartphone)
• Pulsschlag (Erfassung über Armband)
	• Tracking des Nutzerprofils im Internet (zB Cookies)
	  • zu leicht veränderbar
	  • bei Transaktionsrisiko - Analyse wohl zulässig

MaSI – Ausnahmen von der Str. Auth.

1. **White lists** = vertrauenswürdige Begünstigte
   - Definition fehlt; solche, die Vermeidung von Missbrauch gewährleisten
   - Liste im Voraus für den Kunden erstellt, vom Kunden autorisiert

2. Konten **desselben Nutzers** innerhalb **desselben PSP**

3. Konten **unterschiedlicher** Nutzer innerhalb **desselben PSP** nach **Transaktionsrisikoanalyse**

4. **Kleinbetragszahlungen**

Aber immer erforderlich:

Risikoanalyse und deren Dokumenation

MaSI – Auswirkungen für E-Händler I

mittelbare Adressaten

- PSP sollen E-Händler ermutigen, keine sensiblen Zahlungsdaten zu speichern
- wenn diese gespeichert werden, dann bestimmte Sicherheitsmaßnahmen in IT-Infrastruktur, um Datendiebstahl zu verhindern
- PSP muss Umsetzung der Sicherheitsmaßnahmen beim Händler regelmäßig prüfen
- bei Verstößen muss PSP vertragliche Konsequenzen ziehen

MaSI – Auswirkungen für E-Händler II

mittelbare Adressaten

- Wechselseitige Authentifizierung von PSP und E-Händler bei Auslösung von Zahlungen
- Kreditkarte: E-Händler muss Technologie nutzen, die es dem Aussteller ermöglicht, starke Authentifizierung des Kunden zu ermöglichen
- Website des E-Händlers ist angemessen gegen Diebstahl und unbefugten Zugriff oder Änderungen zu sichern
- Zahlungsprozesse klar vom Shop trennen

MaSI – Vertragsanpassungen notwendig?

Vorstellung der BaFin

3.4 Abrechnende Zahlungsdienstleister sollten E-Händler, die sensible Zahlungsdaten speichern, verarbeiten oder übermitteln, vertraglich zur Zusammenarbeit bei schwerwiegenden Zahlungssicherheitsvorfällen, einschließlich Datenschutzverletzungen, mit den abrechnenden Zahlungsdienstleistern selbst und den zuständigen Strafverfolgungsbehörden verpflichten. Erhält ein Zahlungsdienstleister Kenntnis davon, dass ein E-Händler nicht vertragsgemäß kooperiert, sollte er Maßnahmen ergreifen, um diese vertragliche Verpflichtung durchzusetzen, oder den Vertrag kündigen.

MaSI – Auswirkungen bei Outsourcing

mittelbare Adressaten

- PSP lagert Funktionen aus, die Sicherheit der Zahlungsdienste betreffen:

- Outsourcing-Vertrag muss Bestimmungen enthalten, dass MaSI-Anforderungen vom Dienstleister beachtet werden

- bei Neuabschluss beachten, ggf. Vertragsanpassung

SPIRIT LEGAL®

Sabine Fuhrmann
Rechtsanwältin | Partnerin
sabine.fuhrmann@spiritlegal.com

Spirit Legal LLP
0800- 248 2000 (Freecall)

GERMANY
Anwaltshaus im Messehof /// Petersstraße 15 /// D-04109 Leipzig

UNITED KINGDOM
58-60 Kensington Church Street /// London W84DB United Kingdom