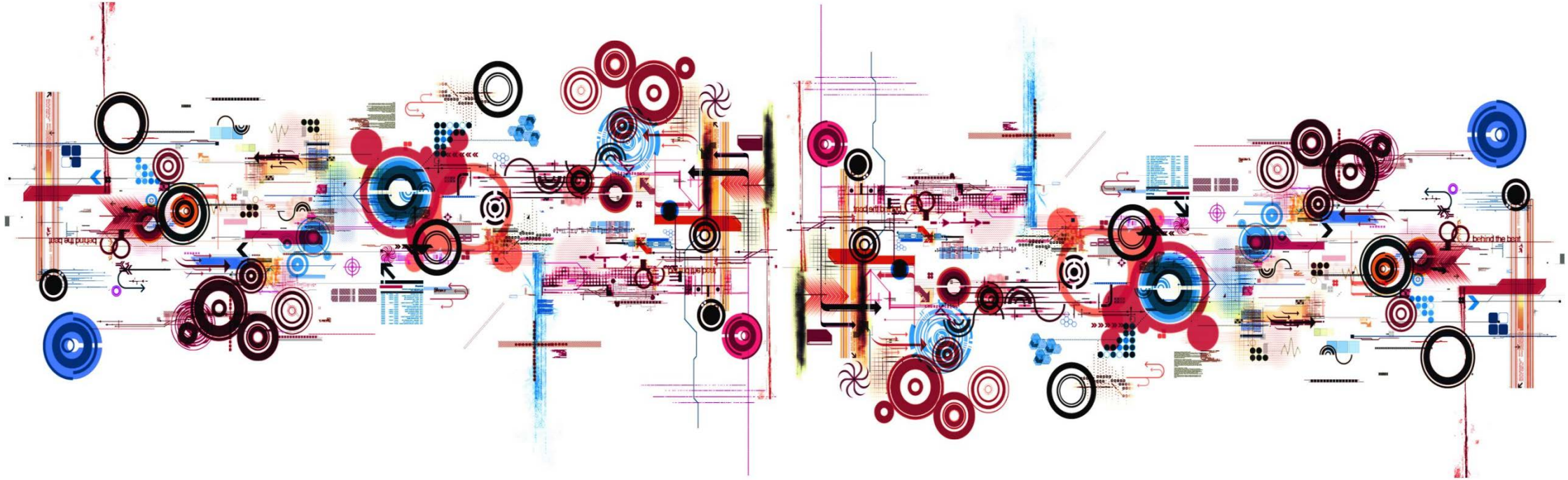
Elektronische Zahlungssysteme aus IT-rechtlicher Sicht

9. Münchner Fachanwaltstag IT-Recht 2019

RA Udo Steger



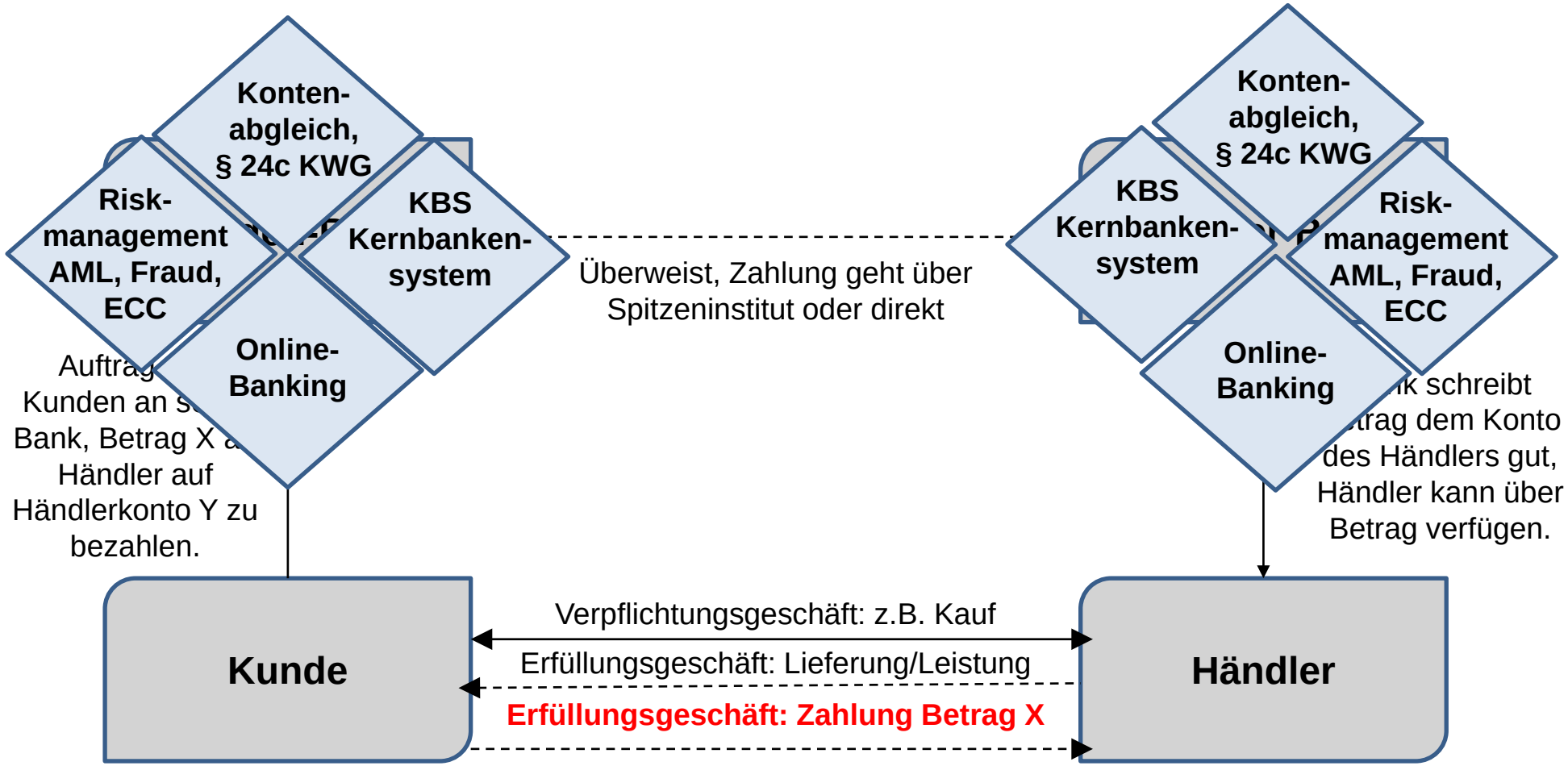
Das Programm für heute

- Zahlungsmethoden im Überblick
  - Grundmodell
  - ELV
  - Kreditkarte
  - Acquirer
- Payment Card Industry Data Security Standard (PCI DSS)
- Aufsichtliche Vorgaben für Bank- und Zahlungsdienste aus IT-rechtlicher Sicht
- Datenschutz – gemeinsame Verantwortlichkeit?

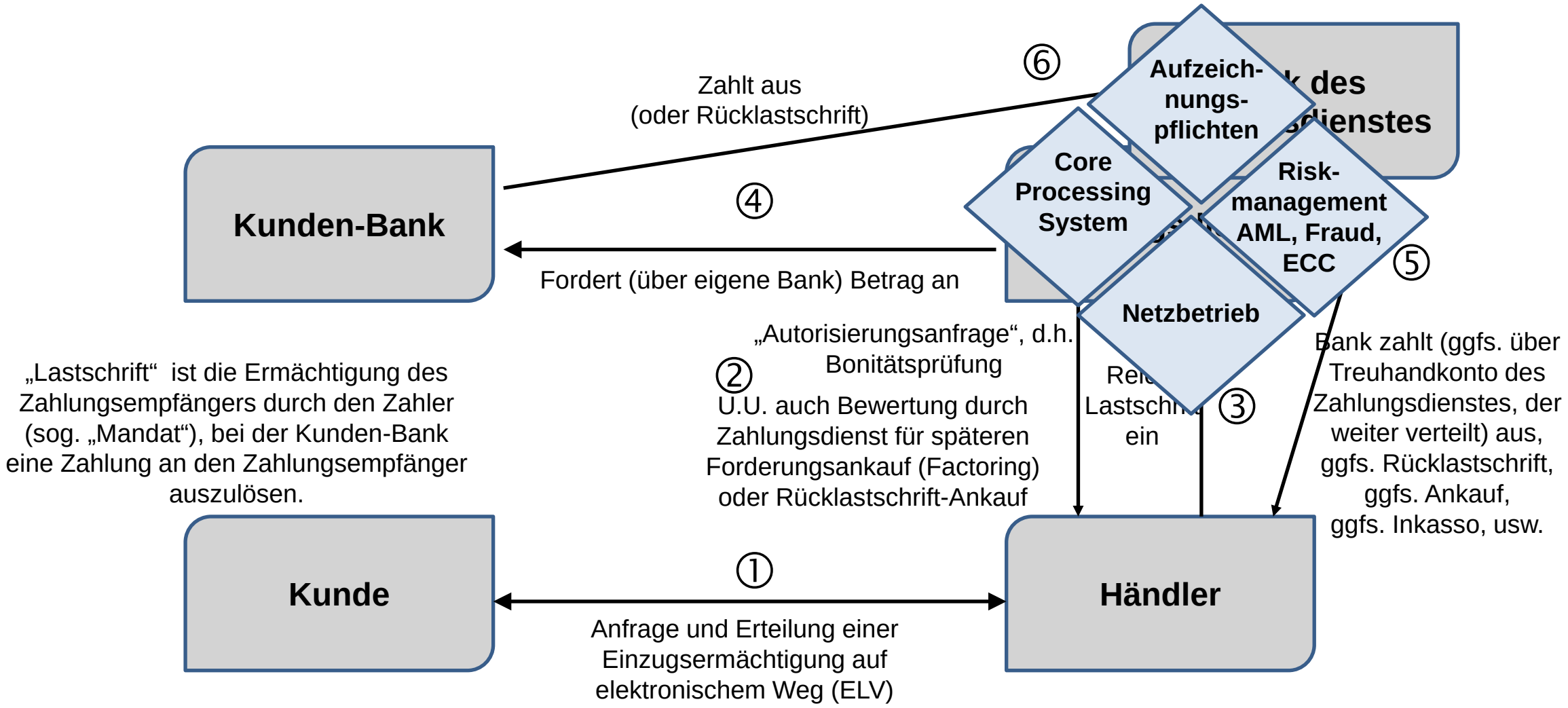
Zahlungsmethoden – Ein Überblick

Technologie	Zahlungsmethode	Anbieter
„Offline“ Zahlungen	Kauf auf Rechnung Vorkasse per Überweisung Teil- oder Ratenzahlungsvereinbarung Bar am POS Alternative bargeldähnliche Verfahren	Händler selbst Bank, bald mit SEPA Instant Payments Händler, Drittanbieter: Klarna, RatePay Händler selbst Paysafecard, Barzahlen.de
kartenbasierte Zahlung	Kreditkarte, Debitkarte Dienste, die über Kreditkarte gefunded werden Spezielle „limited range“ Karten	Mastercard, Visa, Amex, Diner, … Alianz Pay&Protect, Alipay, ggfs. PayPal Tankkarten, Kantinenkarten
nicht-kartenbasierte Zahlung	Lastschrift Überweisung	Elektronische Lastschrift (ELV) Online-Überweisung, auch mittels Payment Initiation Service (PIS)
girokontobasierte Zahlung	Vorkasse p. Überweisung, Lastschrift , Kauf auf Rechnung Dienste, die über Girokonto gefunded werden Peer-2-Peer	Bank PayPal, AliPay PayPal Venmo, MasterCard Moneytou, Kwitt, Square Cash
Wallet, Funding per KK oder Grokonto	digitale Wallet , Mobile Wallet auf Hardware-Basis	Apple Pay, Google Pay, div. Krypto Wallets

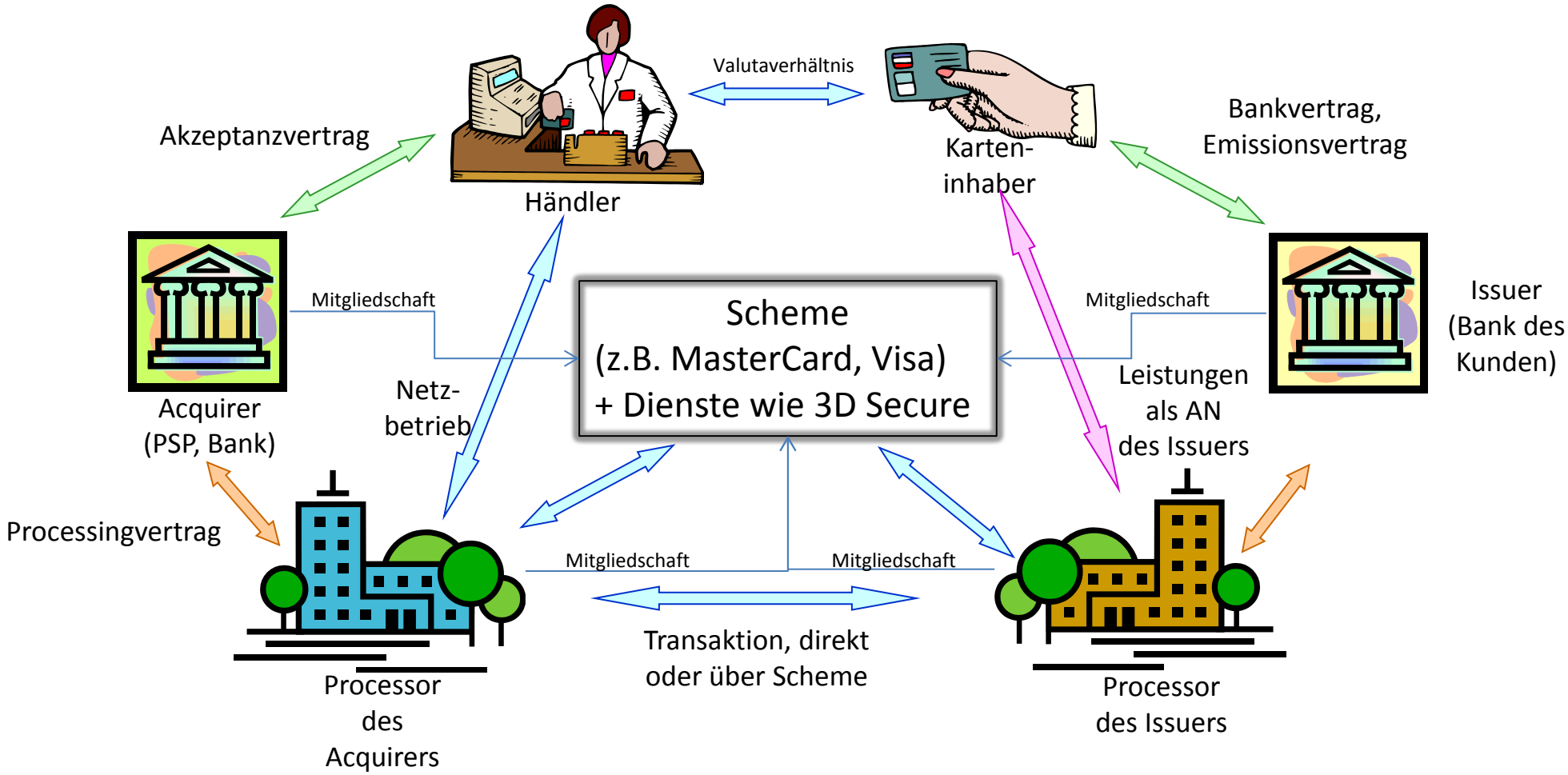
Grundmodell – am Beispiel Überweisung



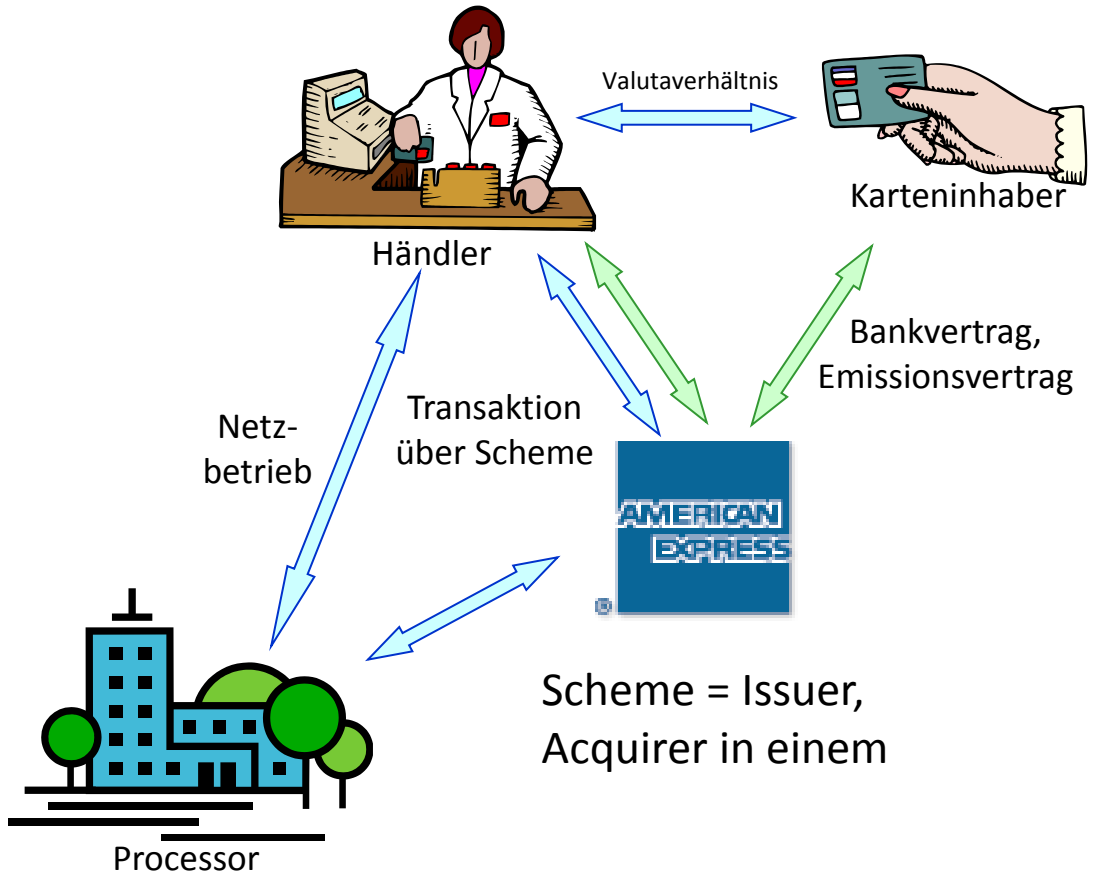
Ablauf elektronische Lastschrift (ELV)



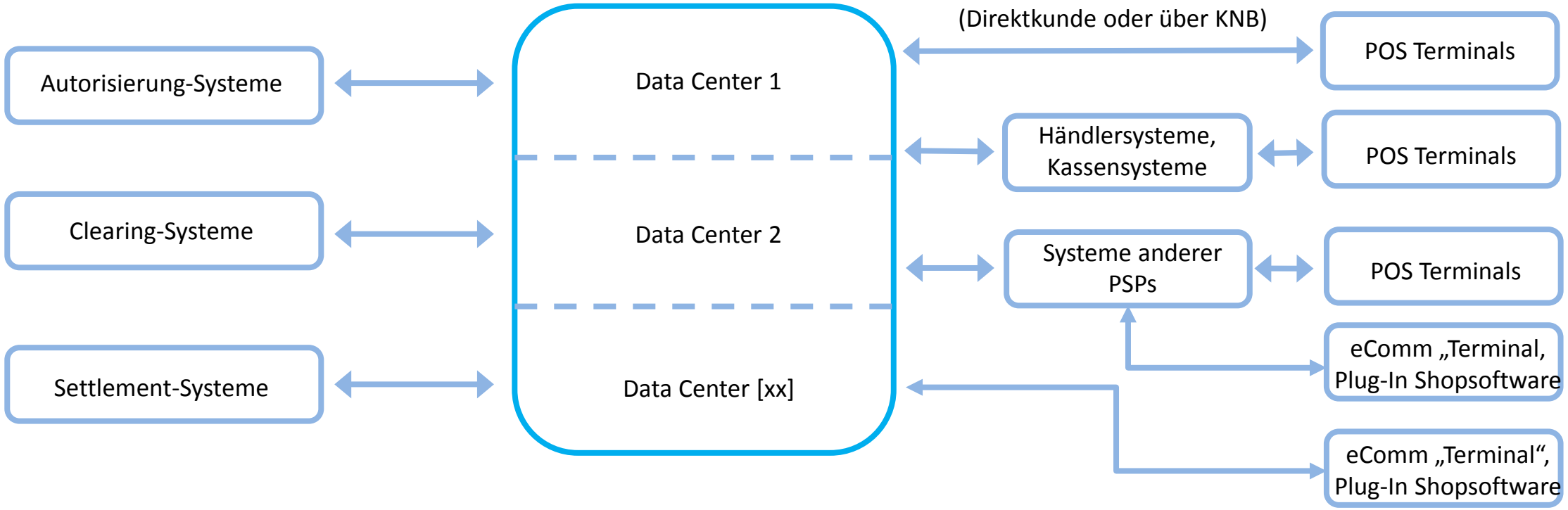
Kreditkartenzahlung – 4-Parteienverhältnis



Kreditkartenzahlung – 3-Parteienverhältnis



Schematische IT-Infrastruktur eines typischen Acquirers



Begriffe aus dem Payment Bereich

- **Autorisierung:**
  Verfahren zur Genehmigung oder Ablehnung von Kartenumsatzanfragen. Die Umsatzanfrage wird durch das Händlerterminal oder den Geldautomaten an die kartenausgebende Bank (Issuer) bzw. das beauftragte Rechenzentrum (Prozessor) gerichtet. Die Antwort kann eine Genehmigung, eine Umsatzablehnung, Aufforderung zum Karteneinzug oder zur Legitimationsprüfung bedeuten.
- **Acquirer**:
  Händlerbank oder Zahlungsdienst, über die der Händler abrechnet
- **Clearing**:
  Clearing meint die Abwicklung der Zahlung (Belastung und Gutschrift des Zahlungsbetrages) zwischen der Händlerbank bzw. dem Acquirer und dem Kartenausgebenden Institut (Issuer)
- **Settlement**:
  Verfahren zur Herbeiführung des gegenseitigen Zahlungsausgleiches zwischen Issuer- und Acquirer-Banken für die pro Tag jeweils abgerechneten Kartenumsätze (einschl. Gebühren). Ein „Nur-Acquirer“ verwendet dazu Konten seiner Bank, die in einem Treuhand-Modell geführt werden (Schutz Händlergelder vor Insolvenz).
- **Kaufmännischer Netzbetreiber (KNB):**
  Der KNB schließt Verträge über Netzbetrieb und Terminals im eigenen Namen und direkt mit den Händlern ab. Die technischen Dienste werden durch einen Netzbetreiber erbracht.

Quelle, und viele Definitionen mehr: https://www.kartensicherheit.de/oeffentlich/glossar.html

Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS)

Branchenstandard zum Schutz von Kreditkartendaten

- entwickelt von den großen Schemes Mastercard, Visa, Amex, Discover, JCB, usw.
- umfaßt 12 generelle technische Vorgaben zum sicheren Umgang mit Kartendaten
  - u.a. Verfahren zur Verschlüsselung, z.B P2P-Encryption bis auf Terminal-Ebene
- Verfahren zur Auditierung, Zertifizierung, und zum Scanning auf Lücken

Gilt für alle, die Kartendaten speichern, verarbeiten oder weiterleiten wollen

- Händler, Acquirer, Terminal-Hersteller, Gateways usw.
- Acquirer sind verpflichtet, alle Händler und PSPs inkl. Zertifizierungsstatus zu registrieren
- Jährliche Validierung

„Super-TOMs“ für die Payment Industrie?

- Ziel ist geschlossenes System für Kreditkartendaten, die nur dorthin gelangen, wo sie hinsollen.
- Auch vielen Parteien (z.B. Händler) wird Zugriff auf die Daten entzogen.

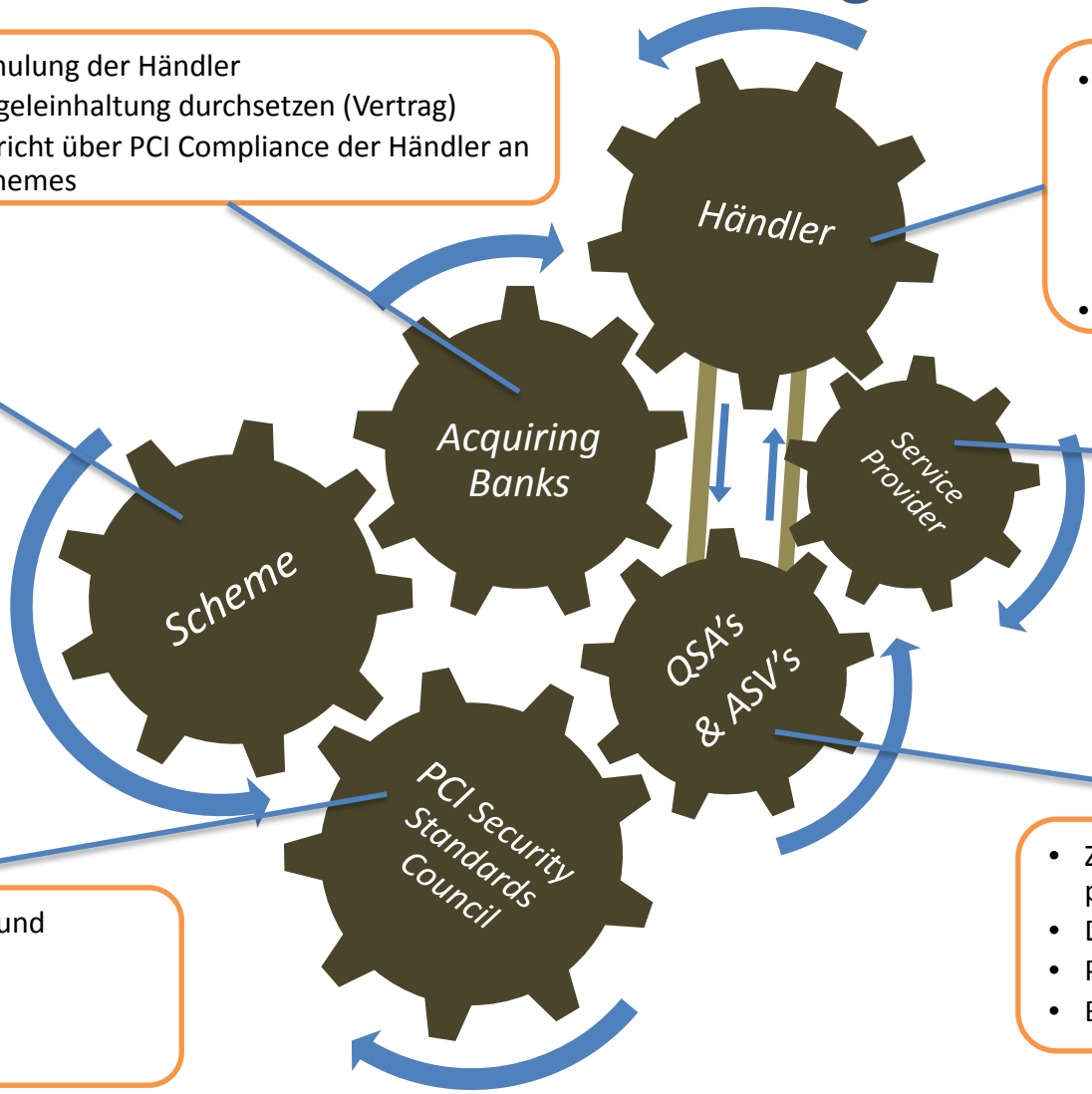
P: PCI DSS vereinbar mit Rolle und Rechten als „Verantwortlicher“ i.S.d. DSGVO?

PCI DSS im Überblick - Vorgaben

Überblick über den PCI-Datensicherheitsstandard

Erstellung und Wartung sicherer Netzwerke und Systeme	1. Installation und Aufrechterhaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten 2. Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
Schutz von Karteninhaberdaten	3. Schutz gespeicherter Karteninhaberdaten 4. Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
Unterhaltung eines Anfälligkeits-Managementprogramms	5. Verwendung und regelmäßige Aktualisierung von Antivirensoftware 6. Entwicklung und Wartung sicherer Systeme und Anwendungen
Implementierung starker Zugriffskontrollmaßnahmen	7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf 8. Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten 9. Physischen Zugriff auf Karteninhaberdaten beschränken
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken	10. Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten 11. Regelmäßiges Testen der Sicherheitssysteme und -prozesse
Befolgung einer Informationssicherheitsrichtlinie	12. Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal

PCI DSS im Überblick – Rollen und Aufgaben



- Schulung der Händler
- Regeleinhaltung durchsetzen (Vertrag)
- Bericht über PCI Compliance der Händler an Schemes

- Pflicht, PCI DSS Vorgaben einzuhalten
  - Umgang mit Kartendaten
  - ggfs. IT-Sicherheit
  - Nutzung zertifizierter Service Provider
- Pflicht zur (Selbst-)Zertifizierung

- Akzeptanz von PCI erhöhen
- Durchsetzung von PCI
  - Strafen bei mangelhafter Umsetzung
  - Sperre wenn fehlt
  - Boni oder höhere Foleranz

- Einhalten der PCI DSS Vorgaben
  - Umgang mit Kartendaten
  - IT-Sicherheit (groß!)
- Pflicht zur Zertifizierung/Auditierung

- PCI DSS Standard fortentwickeln und durchsetzen
- Musterverträge
- Zertifizierung der QSAs und ASVs

- Zertifizierte Prüfer (QSA) für Vor-Ort Audits, prüfen Einhhaltung der PCI DSS Vorgaben
- Durchführen von Vulnerability Scans
- Prüfung von Risikominderungsmaßnahmen
- Berichterstattung

Aufsichtliche Vorgaben aus IT-rechtlicher Sicht

Einige „IT-relevante“ aufsichtliche Anforderungen

- “An der Grenze zum Weltraum”:
  - G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector vom 11.10.2018
  - FinTech-Plan der EU Kommission (8.3.2018), um aufsichtliches Know-How zu verbessern. “EU Fintech Lab” etabliert, 1. Sitzung am 20.06.2018
- Mindestanforderungen an das Risikomanagement (MaRisk, 2017)
  - Einhalten von Standards z.B. des BSI (AT 7.2, Tz. 2)
  - laufende Überwachung (AT 7.2 Tz. 4)
  - Weitergabe der Pflichten beim Outsourcing (AT 9, Tz. 7e)
- Bankaufsichtliche Anforderungen an die IT (BAIT, 2017)
  - Informationsrisikomanagement (II, Tz. 8 – 14)
  - Informationssicherheitsmanagement (II, Tz. 15 – 22)
  - IT-Betrieb (II, Tz. 45 – 51), Auslagerungen (II, Tz. 52 – 56)
  - Besondere Anforderungen für KRITIS (II, Tz. 57-61)

Bisher geltende aufsichtliche Vorgaben

Banken (Zahlungsdienste)

- §25b KWG, § 26 ZAG
- MaRisk
- BAIT
- Orientierungshilfe Cloud

Versicherungen

- § 32 VAB
- MaRisk (VA)
- VAIT

Kapitalverwaltungsgesellschaften

- § 36 KAGB
- KaMaRisk
- KAIT

Neu: Outsourcing-Richtlinie der EBA

Leitlinien zu Auslagerungen – EBA Guideline EBA/GL/2019/02

- gilt für Banken, Zahlungsdienste, E-Geld-Institute, ab 30.09.2019
- Integriert EBA Guideline EBA/REC/2017/03 zu Auslagerungen an Cloud-Anbieter, die dementsprechend aufgehoben wird

Konkretisierung durch BaFin soll in 2020 durch überarbeitete MaRisk erfolgen

- BAIT wird voraussichtlich bleiben

Eine verpasste Chance?

- MaRisk ist bereits lang und komplex
- MaRisk ist Vorbild für MaRisk (VA), KaMaRisk – diese würden auch komplexer
- Auslagerung der IT-bezogenen Themen aus der MaRisk würde diese entlasten (ggfs. um den Preis von Redundanzen)
- „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ vom 8.11.2018 könnte Grundlage sein

Ein paar Eckpunkte, die aufsichtlich beeinflusst werden

- Strategische Überlegungen des Instituts, Risikoanalyse
- Wann liegt „Auslagerung“ vor? Wesentlichkeitsbewertung
- Berücksichtigung von Standards bei Bewertung des Dienstleisters
- Leistungsgegenstand : Beschreibung von Leistungen, Support, Verantwortlichkeiten, Laufzeit, Service Level/KPIs => i.d. Praxis häufig unzureichend/vage
- Informations- und Prüfungsrechte des Instituts und der Aufsicht, keine (mittelbare) Einschränkung der Rechte, Sammelprüfungen, Prüfberichte
- Weisungsrechte des Instituts
- Datensicherheit und Datenschutz
- Redundanz, Ausfallsicherheit, Datensicherheit in der Auslagerungskette
- Absicherung der Wechselmöglichkeit, keine Abhängigkeit
- Weiterverlagerungen

Datenschutz – gemeinsame Verantwortlichkeit?

DSGVO: Gemeinsame Verantwortlichkeit? 1/3

Sind am Zahlungsvorgang Beteilige „gemeinsam Verantwortliche“ (Art. 26 DSGVO)?

- Art. 26 DSGVO: „*Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche…“*
- Art. 4 Nr. 7 DSGVO: „*Verantwortlicher“* [ist] *die … Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet…“*
- Gesetzlicher Tatbestand, der vertraglichen Disposition der Parteien entzogen

z.B. beim Gespann Händler/Acquirer oder Acquirer/Scheme denkbar

- Händler hat beim POS Terminal nur wenig eigenen Einfluss auf Datenverarbeitung
- Schemes geben Acquirern strenge Vorgaben zum Umgang mit Daten, u.a. über PCI DSS

DSGVO gilt auch für Parteien in Nicht-EU Staaten (Art. 3 Abs. 2)

- Ausl. Partei kann „Auftragsverarbeiter“ sein – Art. 28 DSGVO i.V.m. Art. 3 Abs. 1 / 2 DSGVO
- Ausl. Partei kann „Verantwortlicher“ sein – Art. 4 Nr. 7 i.V.m. 3 Abs. 2 DSGVO

DSGVO: Gemeinsame Verantwortlichkeit? 2/3

EuGH: weiter Begriff der „gemeinsamen Verantwortlichkeit“

- Gemeinsame Verantwortlichkeit muss nicht gleichwertige Verantwortlichkeit sein. Verantwortliche können durchaus in unterschiedlichem Ausmaß einbezogen sein. „*Der Grad der Verantwortlichkeit ist unter Berücksichtigung der Umstände des Einzelfalls zu beurteilen*“ (EuGH, Urt. v. 10.7.2018 – Rs. C-25/17)
- Ermöglichung der Verarbeitung durch den anderen Verantwortlichen reicht, Einwirkungsmöglichkeit, Verarbeitung muss (auch) eigenen Zwecken dienen (EuGH, Urt. vom 5.6.2018, Rs. C-210/16)
- Einbindung eines FB „Like“ Button reicht, tatsächlicher Zugriff des gemeinsamen Verantwortlichen ist nicht notwendig (EuGH, Urt. vom 29.7.2019, Rs. C-40/17)

Einige mögliche Konsequenzen:

- es muss Vereinbarung geben, in der die Aufteilung der Pflichten geregelt ist.
- Verzeichnis der Verarbeitungstätigkeiten evtl. unrichtig, Art. 30 Abs. 1 lit. a DSGVO
- Gesamtschuldnerische Haftung gegenüber Betroffenem: Art. 82 Abs. 4 DSGVO
- Bürokratischer Alptraum, wenn Händler oder Acquirer beteiligt wären – und eigentlich immer.

DSGVO: Gemeinsame Verantwortlichkeit? 3/3

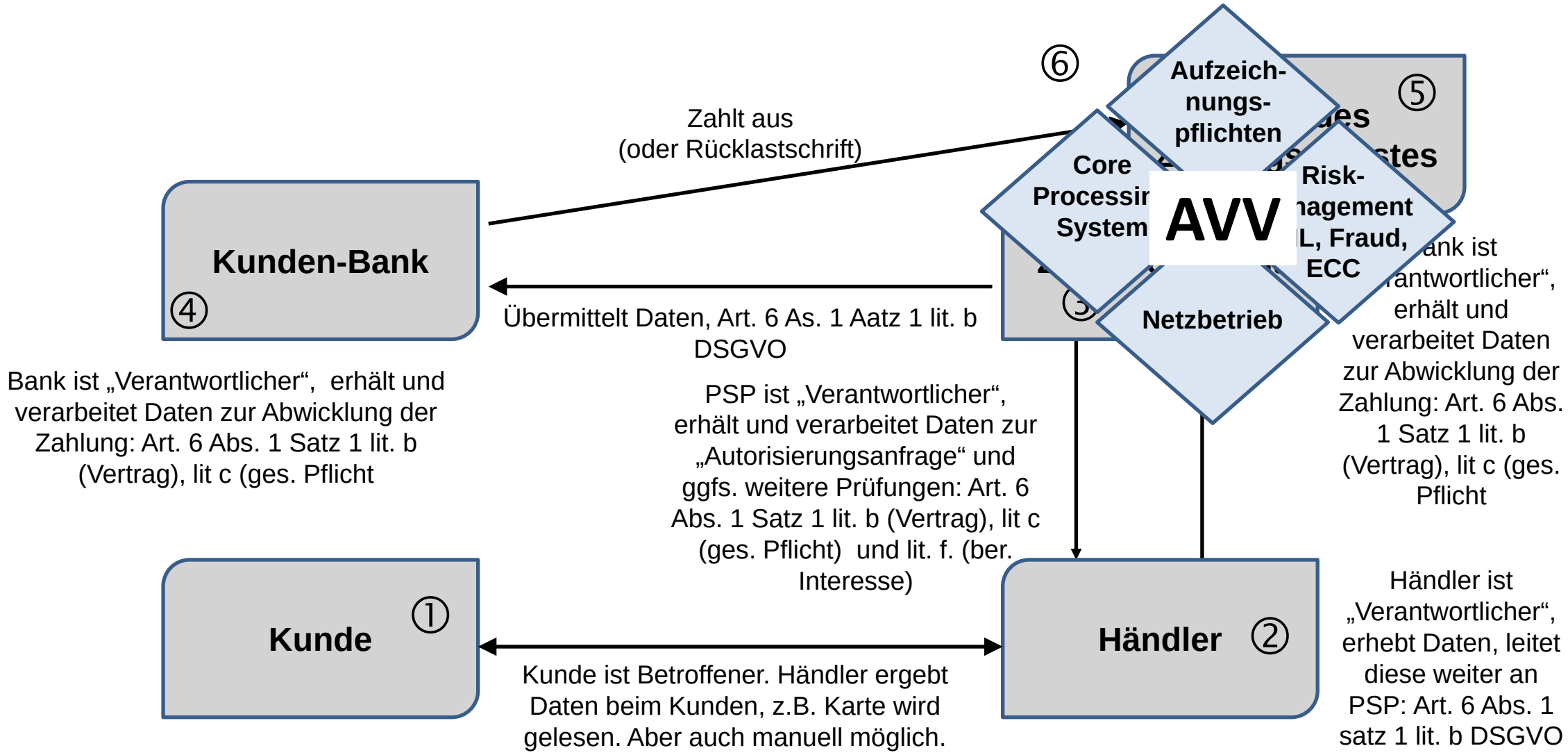
Argumente gegen gemeinsame Verantwortlichkeit:

- Institute sind ist „Verpflichteter“ i.S.d. GwG und müssen alleine über Risikomanagement (§ 4 GwG), Risikoanalyse (§ 5 GwG) und Aicherungsmaßnahmen (§ 6 GwG) entscheiden
- Es darf keine Einschränkung oder Delegation der Verantwortung der Geschäftsleitung geben, auch nicht bei Auslagerung (§§ 25a und 25b KWG, §§ 26 und 27 ZAG)
- Einmischung eines Dritten in erlaubnispflichtige Geschäfte des Instituts könnte Straftatbestand verwirklichen (z.B. § 63 Abs. 1 Nr. 4 ZAG – Zahlungsdienst ohne Erlaubnis)
- Verarbeitungserlaubnis gilt nur für Institute, vgl. § 59 ZAG, §§ 10 Abs. 2, 25h Abs. 2 KWG

Maßnahmen im Payment-Umfeld:

- bei Verträgen strenge Abgrenzung zwischen Händler/PSP, eigenes Verarbeitungsinteresse
- bei Auftragsverarbeitung klare Weisungsrechte des AG, keine Entscheidungsrechte des AN
- präzise Leistungsbeschreibung – wer ist wofür alleine (!) verantwortlich
- Dokumentation durch Verarbeitungsverfahren, in denen nur ein Verantwortlicher vorkommt
- Ggfs. Datenflussdiagramme, die das eigene Verarbeitungsinteresse der Parteien zeigen

DSGVO: Lauter „Verantwortliche“ am Beispiel ELV



Q&A

Vielen Dank!

Udo Steger

Rechtsanwalt / Partner

Aderhold Rechtsanwaltsgesellschaft mbH

Wagmüllerstraße 23

80538 München

Tel.: +49 (89) 306683-270

E-Mail: u.steger@aderhold-legal.de

Follow me:

www.paytechlaw.com