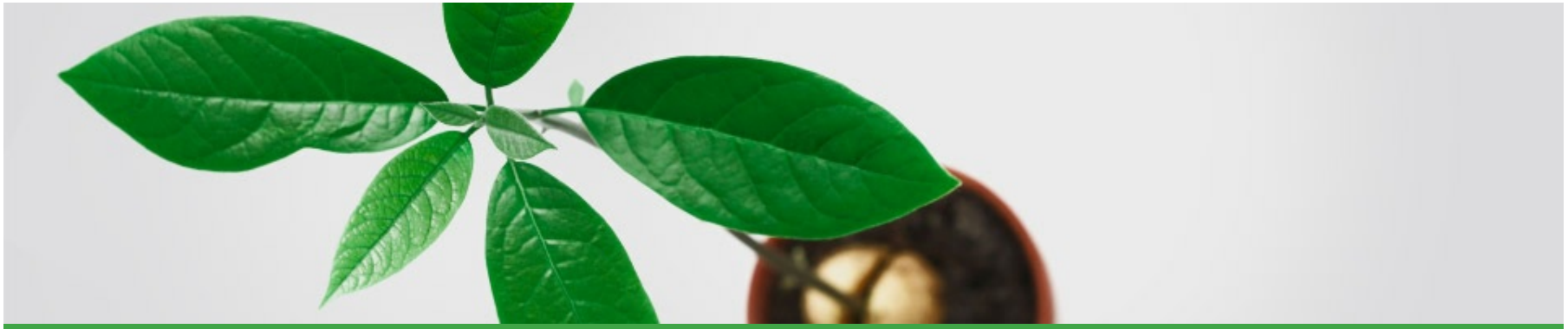
avocado
rechtsanwälte

2. Venture Night, 20.04.2016

Aktuelle Fragen des Datenschutz-Rechts
- vom Cloud Computing über
Safe Harbour bis zur Patientensicherheit

Prof. Dr. Thomas Wilmer, Assessor, Counsel



vitamine für die wirtschaft

Die Welt der Wirtschaft ist voller Chancen und Risiken. Ganz gleich, welches Problem Sie haben oder welche Rechtsfragen Sie bewegen. Wir kennen Ihr Geschäft und tun alles, um es mit Ihrer Hilfe noch besser zu verstehen. Gerne stellen wir unsere Fähigkeiten in Ihre Dienste und finden Lösungen und Strategien für Ihren Erfolg.

Unser Netzwerk ist groß und weit verzweigt. Wir sind mit rund 50 Anwälten und 75 weiteren Mitarbeitern an den deutschen Wirtschaftsstandorten und in Brüssel tätig. Dank internationaler Kooperationen mit führenden ausländischen Kanzleien können wir Sie auch im Ausland beraten.

Haben Sie alles schon einmal gehört? Und doch gibt es einen Unterschied. Unsere Partner und Mitarbeiter sind auf ihrem jeweiligen Fachgebiet ausgewiesene Experten mit Kompetenz und Erfahrung. Trotzdem ist jeder von uns noch genauso neugierig und unvoreingenommen, wie am Anfang seiner Anwaltskarriere. So nutzen wir unser kreatives Potenzial in Ihrem Interesse.

avocado rechtsanwälte werden von JUVE HANDBUCH WIRTSCHAFTSKANZLEIEN 2014/2015 und LEGAL500 (Directory of Law Firms) sowie Kanzleien in Deutschland empfohlen u.a. für Gesellschaftsrecht und M&A, Arbeitsrecht, IT und Outsourcing, Datenschutz, gewerblicher Rechtsschutz, Telekommunikation, Bankrecht, Immobilienwirtschaftsrecht, Öffentliches Recht und Prozessführung.

The LEGAL 500 EMEA LEADING FIRM 2012

JUVE www.juve.de

anwälte, die ihr geschäft verstehen.

Die meisten rechtlichen Probleme und deren optimale Lösung erschließen sich erst dann, wenn man das betroffene Unternehmen und dessen Geschäft gut kennt. Wir wollen Ihre Probleme verstehen und lösen. Deshalb interessiert uns Ihr Geschäft. Unsere Anwälte arbeiten seit vielen Jahren für in ihrem jeweiligen Sektor marktführende Unternehmen sowie Industrieverbände und sind Experten für die entsprechenden Branchen und Märkte.

. automotive

. banken, versicherungen, finanzdienstleister

. pharma, chemie, rohstoffe

. energie

. entsorgung

. freizeit, sport, kultur

. immobilien, bau

. lebensmittel, konsumgüter, einzelhandel

. medien, telekommunikation, technologie

. transport, logistik, infrastruktur

fachbereiche

Das Wirtschaftsleben ist ebenso spannend wie komplex. Gesetze und Verordnungen ändern sich schnell. Deshalb bauen
wir auf unsere spezialisierten Anwälte, die in permanentem Kontakt stehen und wertvolle Erfahrungen und Fachwissen austauschen. Unsere Mandanten profitieren von dieser Kompetenz auf allen Rechtsgebieten. Dabei versteht es sich von selbst, dass wir unser Wissen ständig aktualisieren und erweitern, um Ihnen eine Rechtsberatung auf höchstem Niveau zu garantieren.

. allgemeines wirtschaftsrecht und konfliktlösung
. arbeitsrecht
. banken und finanzen
. bau und immobilienwirtschaft
. geistiges eigentum, medien und informationstechnologie
. m&a, gesellschafts- und steuerrecht
. notariat
. öffentliches wirtschaftsrecht
. strafrecht

geistiges eigentum, medien und informationstechnologie

Unsere Experten des Fachbereichs "Geistiges Eigentum, Medien und Informationstechnologie“ (neun Berufsträger) sind Ihre Ansprechpartner in allen folgenden Arbeitsgebieten:

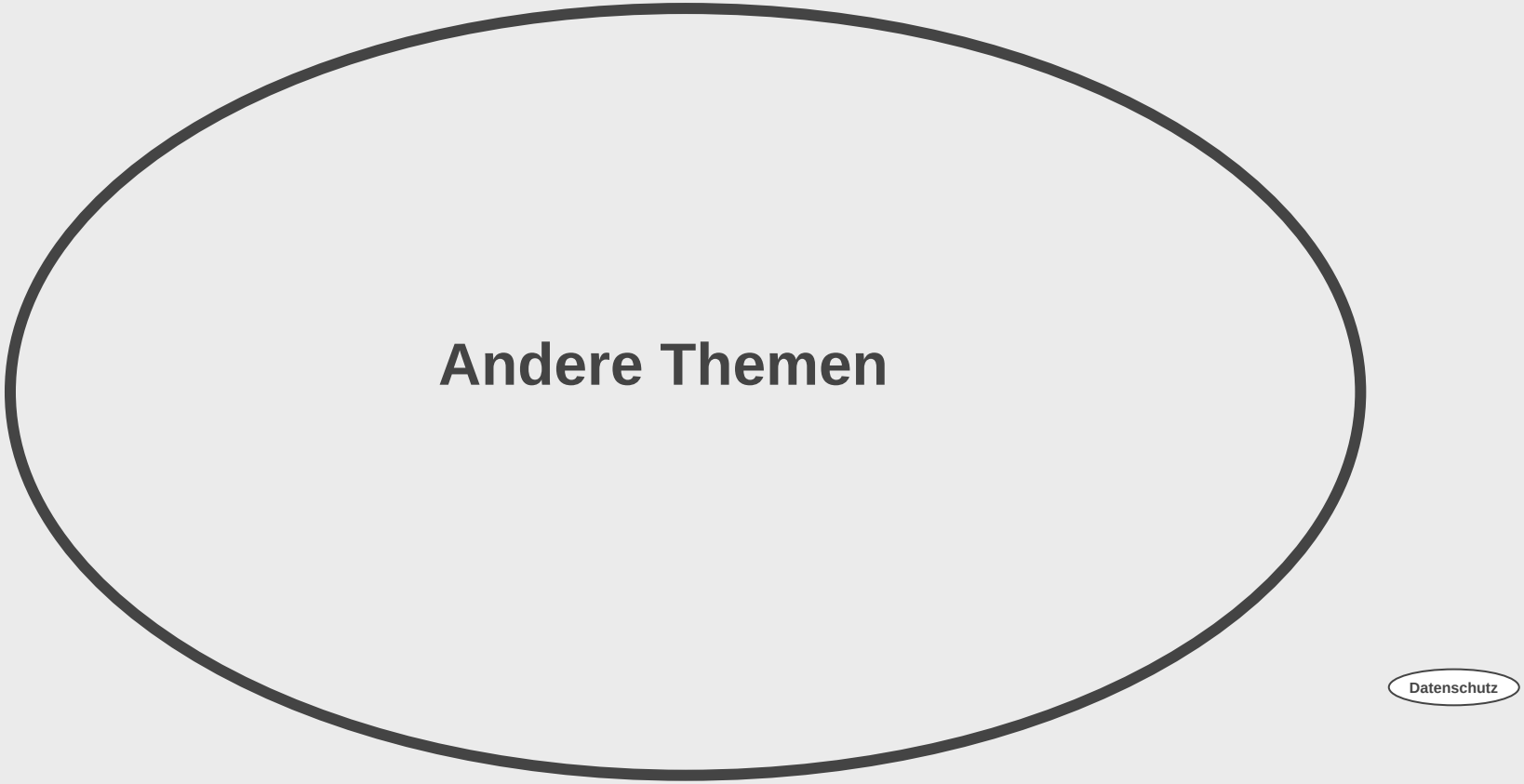
. Computerrecht
. Datenschutzrecht
. E-Commerce
. EDV-Recht
. Film und Entertainment
. Gebrauchsmusterrecht
. Informationstechnologie
. IT-Recht
. Markenrecht
. Medienrecht
. Patentrecht
. Presse und Verlage
. Presserecht
. Rundfunkrecht
. Telekommunikation
. Unlauterer Wettbewerb
. Urheberrecht
. Vertriebsrecht
. Werberecht
. Wettbewerbsrecht

Themenübersicht

Themen

- Kurze Einführung
- Internationaler Datentransfer / Änderungen durch EU-US Privacy Shield
- Cloud Computing
- Beispiel Patientendaten
- Verletzungsfolgen / Maßnahmen der Datenschutzaufsicht

Einführung: Bedeutung des Datenschutzes für Unternehmen früher



Einführung

Begrifflichkeiten und Entstehungsgeschichte

„Jeder muss wissen, wer was wann wo und bei welcher Gelegenheit über ihn weiß.“

Ich muss daher unter anderem wissen (können):

- Wem habe ich meine Daten gegeben?
- Zu welchem Zweck?
- An wen wurden die Daten weitergegeben?
- Wurden sie verändert?
- Wann werden sie gelöscht?

Einführung

Begrifflichkeiten:

- Allgemeines Persönlichkeitsrecht
- Personenbezogene Daten,
- besondere Personenbezogene Daten

Im weiteren Sinne – insbesondere im Unternehmenbereich:

- Geheimnisschutz,
- Vertrauliche Daten aufgrund NDA
- Eigenes Know-How

Einführung

Wer hat woher meine Daten?

Beispiel: Eine Fluggesellschaft veräußert die Daten

- der Vielflieger, die
- männlich sind und
- auch auf Kurzstrecken
- immer Gangplätze gebucht haben
- und über 50 Jahre alt sind

aber an wen?...

Einführung

Begrifflichkeiten: Was sind **personenbezogene Daten?**

§ 3 Abs. 1 „Einzelangaben über

persönliche oder sachliche Verhältnisse
einer bestimmten oder
bestimmbaren (mit vertretbarem Aufwand ermittelbaren)
natürlichen Person“

„GesamtIQ des 4-köpfigen Teams bei 350“ (Verfügbares Zusatzwissen !)
Patienternfallakte?
Daten oder auch Kommentare von Kollegen?
Der Name einer Person selbst?
Die Adresse einer Person?

Einführung

Begrifflichkeiten: **Besondere Personenbezogene Daten**:

§ 3 (9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Werden religiösen Daten werden im Krankenhaus erfasst?

Mögliche Zwecke?

Einführung

Umgang mit Daten: Wann zulässig?

Grundregel:

§ 4 BDSG Zulässigkeit der Datenverarbeitung und -nutzung

Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig,
wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

§ 4a BDSG

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Datenschutzfragen beim internationalen Datentransfer

Haarsträubend unübersichtliche Lage

„EU-US Privacy Shield ist Lückenfüller“

„EU-US Privacy Shield: starke und robuste Datenschutzregelung“

„Schild zur Abwehr der Verantwortung“

„Erstmals bindende Zusagen der USA“

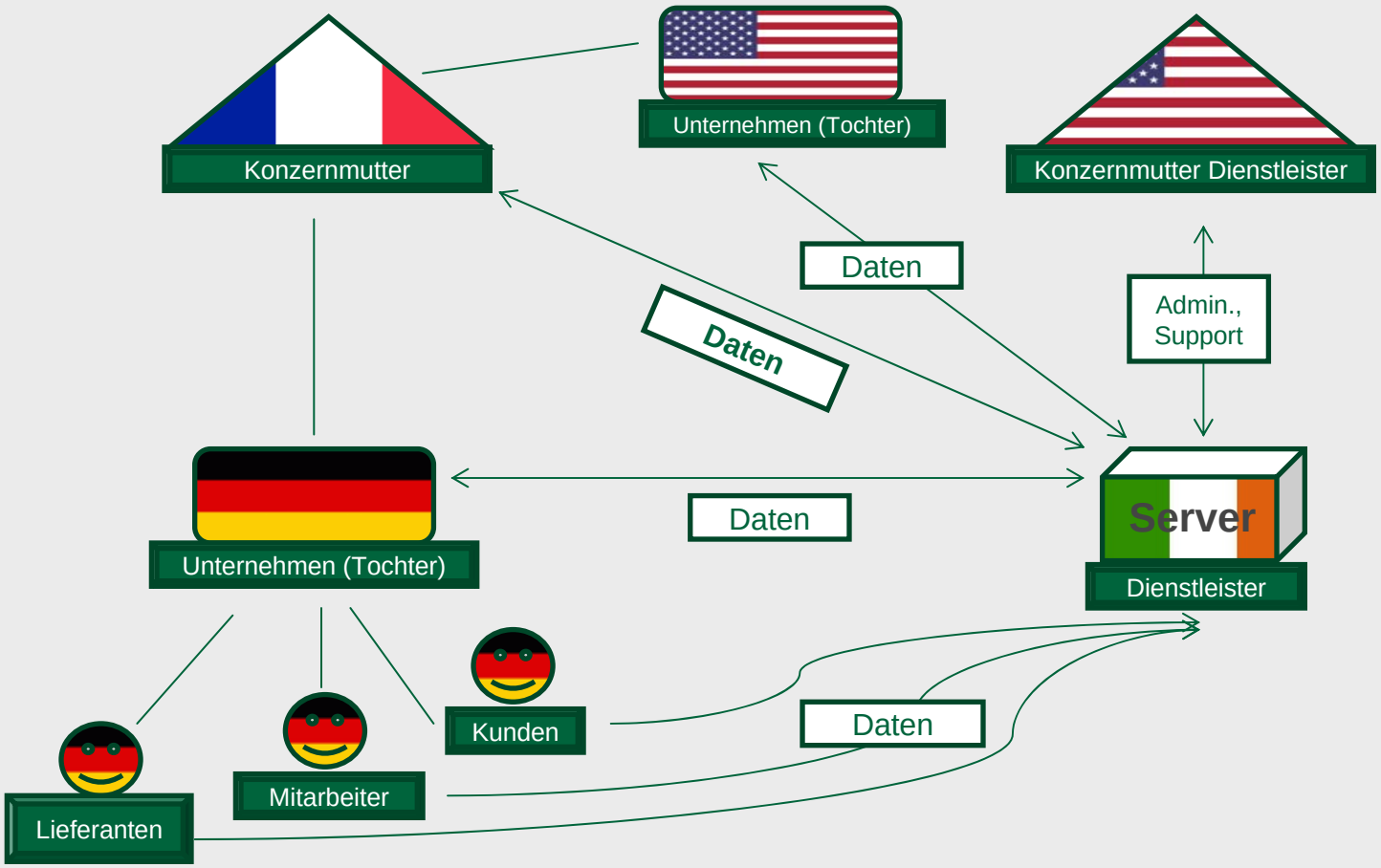
„Verschleierungs-trick“

„Details abwarten und dann prüfen“

„Keine Massenüberwachung mehr“

Datenschutzfragen beim internationalen Datentransfer

Beispiel 1: Datenströme bei konzernweitem CRM-System



Internationaler Datentransfer – rechtliche Voraussetzungen

a) EU- und EWR-Staaten, Drittstaaten

- Internationaler Datentransfer entspricht Datentransfer innerhalb Deutschlands (identische Voraussetzungen):
  - EU- und EWR-Staaten
  - Drittländer mit angemessenem Datenschutzniveau (sog. Angemessenheitsentscheidungen d. EU-Kommission):

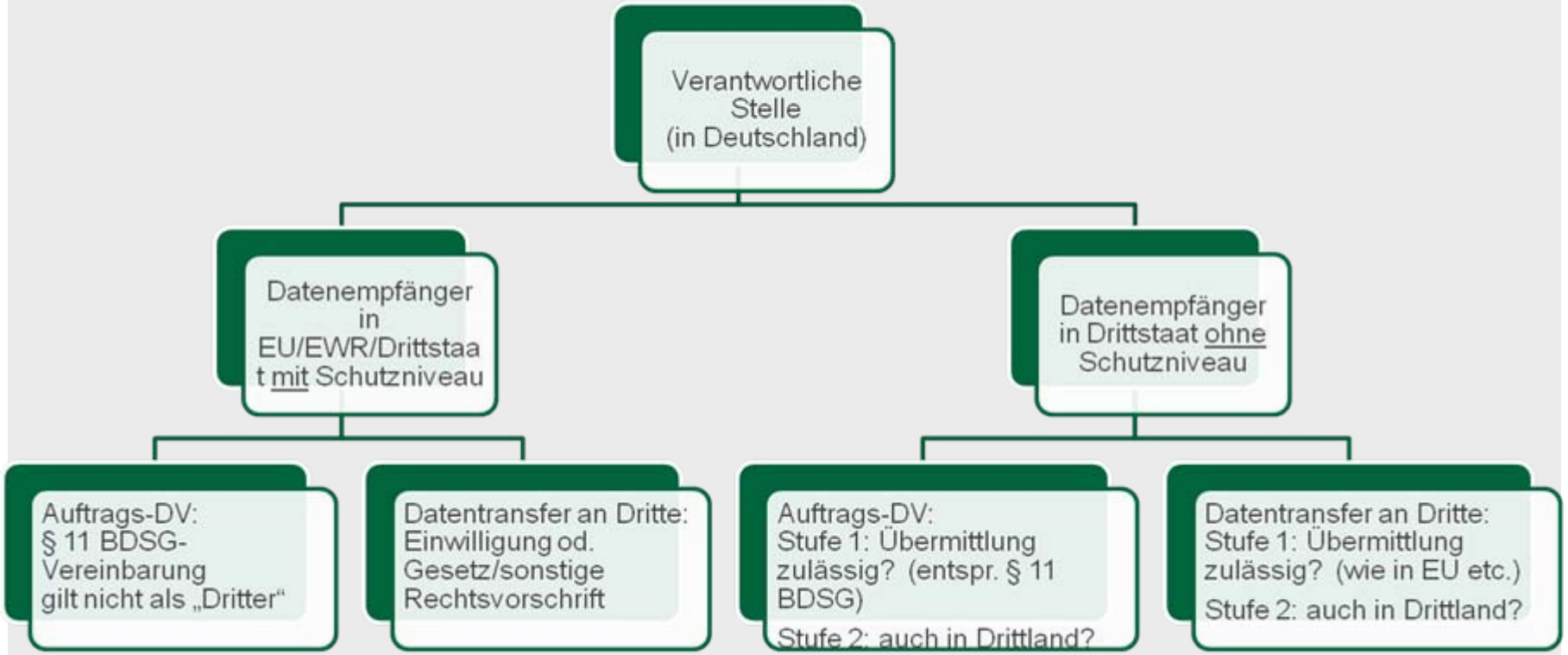
    Andorra, Argentinien, Färöern, Guernsey, Isle of Man, Israel, Jersey, Kanada (nur f. best. Daten), Neuseeland, Schweiz, Uruguay

- Besondere Anforderungen an Datentransfer:
  - Drittländer ohne angemessenes Datenschutzniveau

    => alle anderen Staaten, so auch die USA

Internationaler Datentransfer – rechtliche Voraussetzungen

b) Datentransfer in Drittstaaten - Prüfungsstufen



Internationaler Datentransfer – rechtliche Voraussetzungen

c) Datentransfer in Drittstaaten, Erlaubnis gemäß des § 4c BDSG?

Erlaubnis	Voraussetzungen	Schwierigkeit
Einwilligung	Umfangreiche Informationserteilung, Freiwilligkeit	Praktisch oft nicht umsetzbar, Widerrufsrecht d. Betroffenen
Erforderlichkeit der Übermittlung	Vertragserfüllung, vorvertr. Maßn. auf Veranlassung d. Betroffenen oder in dessen Interesse	Veranlassung d. Betroffenen? Im Interesse d. Betroffenen?
	Wichtiges öffentliches Interesse / Gerichtsverfahren	Bei CRM etc. nicht einschlägig
	Wahrung lebenswichtiger Interessen d. Betroffenen	Bei CRM etc. nicht einschlägig
Übermittlung aus öffentlichem Register	Branchenbücher etc. (BZR, Schuldnerverzeichnis usw. nur bei berechtigtem Interesse d. Empfängers)	Bei CRM etc. i.d.R. nicht einschlägig
Einzelfallbezogene Ausnahmegenehmigung durch Aufsichtsbehörde	Ausreichende Garantien zum Schutz d. Persönlichkeitsrechte auf Seiten der Empfängerstelle	Anfechtbar durch Betroffene, Verfahrensdauer, => geringe praktische Relevanz

Internationaler Datentransfer – rechtliche Voraussetzungen

d) USA: Erlaubnis gemäß „Safe Harbor“?

- Safe Harbor Vereinbarung zwischen EU u. USA, Juli 2000:
  - Datentransfer an Safe Harbor registrierte US-Unternehmen zulässig

- **Zusätzliche Anforderungen** der deutschen Datenschutzaufsicht („**2010/2015-Ergänzung**“):
  - **Nachweis** d. Safe Harbor-Selbstzertifizierung und d. Einhaltung d. Grundsätze, insbes. d. Informationspflichten (Düsseldorfer Kreis, April 2010)
  - **Garantie**, dass staatliche Zugriffsmöglichkeiten auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben (Entschl. d. Konf. d. Datenschutzbeauftragten d. Bundes u. d. Länder, März 2015)

- Urteil des EuGH (Schrems ./. Facebook), Oktober 2015:
  - Safe Harbor Vereinbarung unwirksam, kein angemessenes Datenschutzniveau

=> **Keine Erlaubnis des Datentransfers in die USA gemäß Safe Harbor**

Internationaler Datentransfer – rechtliche Voraussetzungen

e) EU-Standardvertragsklauseln – Controller to Controller

- Datentransfer an eine eigenverantwortliche Stelle („Controller to Controller“):
  - Stufe 1: Prüfung, ob Datenübermittlung an Dritten überhaupt zulässig ist
  - Stufe 2: Zulässigkeit des Datentransfers ins Ausland durch Vereinbarung der EU-Standardvertragsklauseln

- **Set I** der EU-Standardvertragsklauseln (2001):
  - Gesamtschuldnerische Verpflichtung beider Controller ggü. Betroffenen, Datenschutzgrundsätze sicherzustellen
  - Beachtung d. Feststellungen/Ratschläge d. Aufsicht durch Datenimporteur

- **Set II** der EU-Standardvertragsklauseln (2004, flexibler, wirtschaftsfreundlicher):
  - Keine gesamtschuldnerische Verpflichtung wie bei Set I
  - Beachtung nur von bestandskräftigen u. verbindlichen Entscheidungen d. Aufsicht
  - Deutsche Aufsichtsbehörden: Set II ungeeignet f. Arbeitnehmerdaten!

    => Anpassung Set II (Auskunft, Berichtigung, Löschung u. Schadensersatz)

Internationaler Datentransfer – rechtliche Voraussetzungen

f) EU-Standardvertragsklauseln – Controller to Processor

- Datentransfer an einen weisungsabhängigen Auftragsdatenverarbeiter („Controller to Processor“):
  - EU-Standardvertragsklauseln „Controller to Processor“ (Fassung v. 05.02.2010)
  - Auftragsdatenverarbeiter gilt nicht als „Dritter“,

    => keine Prüfung erforderlich, ob Datenübermittlung an Dritten überhaupt zulässig

- Vertragsparteien:
  - Data Exporter (Controller) innerhalb EU/EWR
  - Data Importer (Processor) außerhalb EU/EWR

- Notwendige Ergänzungen gemäß § 11 II BDSG:
  - Umfang, Art u. Zweck der Datenverarbeitung
  - Unteraufträge
  - Weisungsbefugnisse
  - Berichtigung, Löschung und Sperrung von Daten

Internationaler Datentransfer – rechtliche Voraussetzungen

g) Binding Corporate Rules („BCR“) für konzerninternen Datentransfer

- Verbindlichkeit der BCR:
  - Verbindlichkeit nach innen und außen (Durchsetzbarkeit)
  - Mehrseitiger Vertrag, Drittbegünstigung (Intra-Group-Agreement)
  - Alternative: Konzernrichtlinie (Problem: Verbindlichkeit nach außen?)
  - Alternative: Einseitige Verpflichtungserklärung (Problem: nicht in jeder Rechtsordnung anerkannt)
  - Einbeziehung in Arbeitsverträge / Direktionsrecht

- Bestandteile u.a.:
  - Anwendungsbereich, Definitionen, Datenschutzgarantien
  - Auftragsdatenverarbeitung innerhalb u. außerhalb d. Konzerns
  - Konflikte mit nationalem Recht
  - Sicherstellung d. Befolgung, Drittbegünstigung, Haftung

- Behördliche Anerkennung (Mutual Recognition-Verfahren)

Internationaler Datentransfer - Änderungen durch EU-US Privacy Shield

a) Presseerklärung d. EU Kommission vom 29.02.2016

- EU-US Privacy Shield ist Grundlage einer Adäquanzentscheidung
- Soll EuGH-Vorgaben vom 06.10.2015 einhalten
- Grundlagen der Anerkennung
  - Keine willkürliche massenhafte Überwachung
  - Verbesserung der Betroffenenrechte
  - Ombudsmann im Handelsministerium
  - Federal Trade Commission kontrolliert Unternehmen strenger
  - Veröffentlichung Unternehmensrichtlinien
  - Beachtung europäischer Vorgaben
- FAQ: http://europa.eu/rapid/press-release_MEMO-16-434_en.htm

Internationaler Datentransfer - Änderungen durch EU-US Privacy Shield

b) Konkretes Prozedere

- US-Unternehmen registrieren sich
- Selbstzertifizierung
- Jährliches Update
- 45 Tage-Reaktionsfrist auf Beschwerden
- Kooperation mit europäischer Datenschutzaufsicht
- Teilnahme an „Alternative Dispute Resolution“
- EU-US Umbrella Agreement

c) Was sagt Art. 29 WP?

- Pressemitteilung vom 13.04.2016 :

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf

- Stellungnahme vom 13.04.2016:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

- Stellungnahme hierzu von BfDI vom 13.04.2016:
  http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2016/07_NachbesserungsbedarfPrivacyShield.html

c) Was sagt Art. 29 WP?

- Verbesserungen gegenüber Safe Harbor:
  - Schlüsseldefinitionen
  - Transparenz der Teilnehmerunternehmen
  - internen und externen Kontrollmaßnahmen

- Bedenken:
  - kommerzielle Aspekte
  - Datenzugriff durch Behörden
  - Zweifel an Unabhängigkeit des Ombudsmanns als Kontrollinstanz
  - Unübersichtlichkeit und Inkonsistenz der Dokumente zum Privacy Shield (insbesondere beim Zweckbindungsgrundsatz)
  - praktische Probleme bei Beschwerdemöglichkeiten der Betroffenen (Komplexität, Sprachbarrieren)
  - noch zu prüfende Übereinstimmung mit den Prinzipien der EU-DSGVO

Internationaler Datentransfer - Änderungen durch EU-US Privacy Shield

c) Was sagt Art. 29 WP?

- Schlussfolgerungen der Art. 29 WP:
  - EU-Kommission wird aufgefordert, die entsprechenden Bedenken zu berücksichtigen und bei den weiteren Verhandlungen die erforderlichen Anpassungen in der Adäquanzentscheidung vorzunehmen.
  - Bis auf Weiteres bleiben EU-Standardvertragsklauseln und Binding Corporate Rules zulässiges Mittel des Datentransfers (vgl. Seite 32 d. Art. 29 WP Stellungnahme vom 13.04.2016).
- Konsequenzen:
  - Stellungnahme d. Art. 29 WP nicht bindend für EU-Kommission
  - Datenschutzaufsichten erwägen Überprüfung durch EuGH

Internationaler Datentransfer - Änderungen durch EU-US Privacy Shield

d) Was sagen datenschutzrechtliche Aufsichtsbehörden?

- Aktuelle Informationen aus den deutschen datenschutzrechtlichen Aufsichtsbehörden:
  - Safe Harbor alleine führt zu Sanktionen, auch mit 2010/2015-Ergänzung
  - Noch offen, ob 2010/2015-Ergänzungen auch für EU-US Privacy Shield fortgelten
  - EuGH könnte EU-US Privacy Shield für unwirksam halten
  - „Schonfrist bis Juni 2016“ / „keine Endfrist“
  - BfDI begrüßt Stellungnahme d. Art. 29 WP (s. Stellungnahme hierzu von BfDI vom 13.04.2016)
  - In der Praxis maßgeblich: datenschutzrechtliche Aufsichtsbehörden!

Internationaler Datentransfer - Änderungen durch EU Datenschutzgrundverordnung („EU-DSGVO“), gültig ab 2018

- Auslandsdatentransfer:
  - Grundsatz des angemessenen Schutzniveaus bleibt bestehen
  - Keine grundsätzlichen neuen Privilegierungen
  - Art. 44ff. EU-DSGVO:
    - Art. 45 Angemessenheitsbeschluss
    - Art. 46 Datenübermittlung auf der Grundlage geeigneter Garantien, u.a. Standarddatenschutzklauseln
    - Art. 47 BCR
    - Art. 49 Sonderfälle
      - Einwilligung
      - Vertragserfüllung
      - Besondere Interessen (aber Einschaltung Aufsicht)

Internationaler Datentransfer - Änderungen durch EU Datenschutzgrundverordnung („EU-DSGVO“), gültig ab 2018

Konzerndatentransfer:

- Bisher

§ 28 II Nr. 2 BDSG: „Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig, soweit es erforderlich ist, zur Wahrung berechtigter Interessen eines Dritten und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.“

- Neu

Erw. (48): „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe **für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten**, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt. “

Folgen Safe Harbor - Empfehlungen

a) Verträge – bestehende Vereinbarungen

- Änderungsansprüche ?
  - Enthält Vertrag Klauseln mit Anpassungspflichten?
  - Vertragliche Nebenpflicht, § 241 II BGB („Rücksichtspflicht“)
  - Störung der Geschäftsgrundlage, § 313 BGB
  - Einschaltung der Aufsichtsbehörden (anonym)
- Safe Harbor „Migration“ zu EU-US Privacy Shield?
  - Derzeit noch nicht wirksam vereinbart (nicht vor Ende Juni 2016)
  - Kein „automatischer Wechsel“ von Safe Harbor auf EU-US Privacy Shield
  - Datenschutzrechtliche Aufsichtsbehörden lassen EU-US Privacy Shield derzeit nicht genügen
  - Unklar, ob ggf. entsprechende Änderungen verhandelt werden

  => EU-US Privacy Shield zur Zeit keine Lösung

Folgen Safe Harbor - Empfehlungen

a) Verträge – neu abzuschließende Vereinbarungen

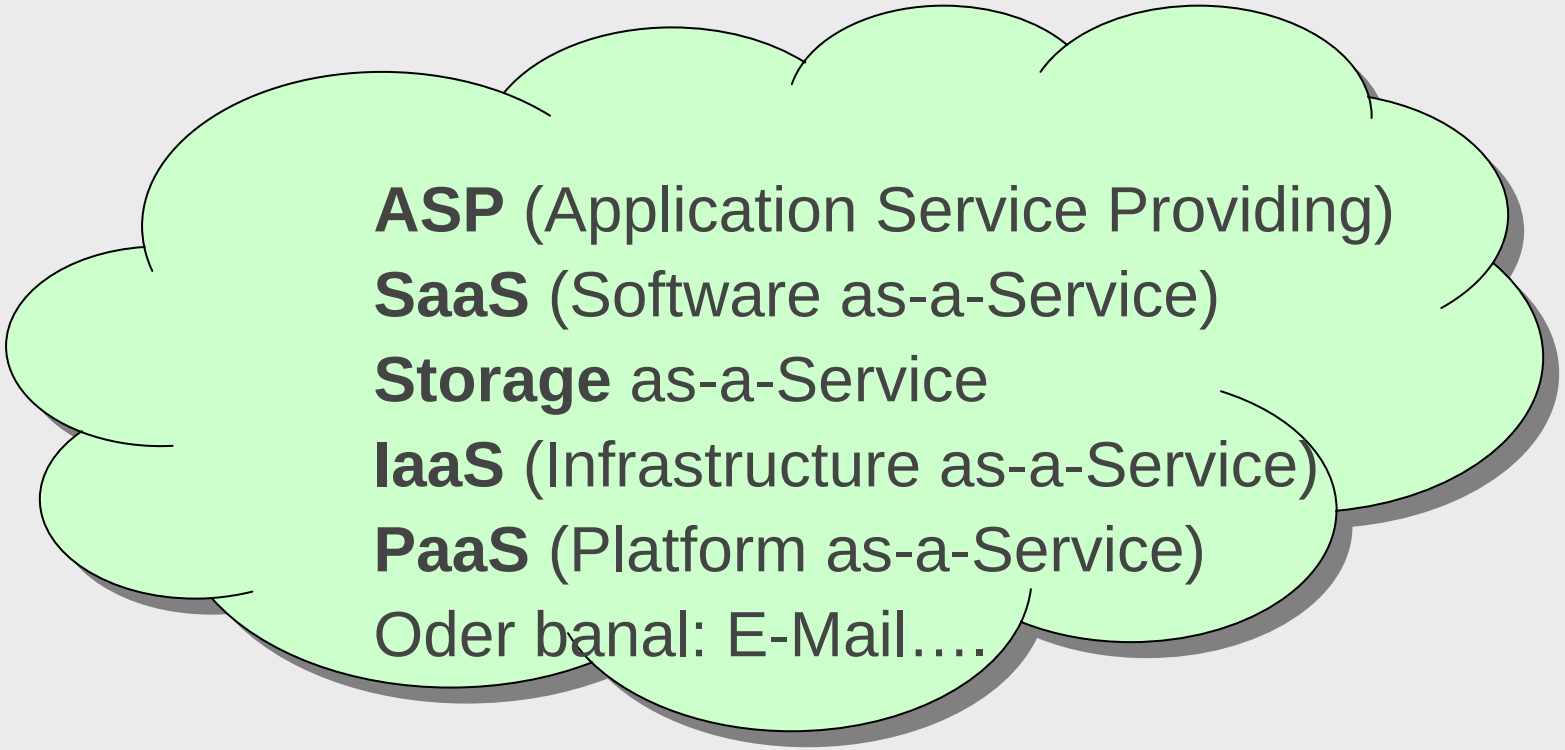
- Empfehlungen der Aufsichtsbehörden:
  - BCR und EU-Standardvertragsklauseln verwenden oder
  - Speicherung nur innerhalb EU/EWR (z.B. auch: „Datentreuhand“)
- Klauseln mit Anpassungspflichten in den Vertrag aufnehmen:
  - Beachtung EU-US Privacy Shield
  - Verpflichtung zur Anpassung an alle Vorgaben
    - Nicht nur Art. 29 WP, sondern
    - Düsseldorfer Kreis und
    - Zuständige Aufsichtsbehörde

Folgen Safe Harbor - Empfehlungen

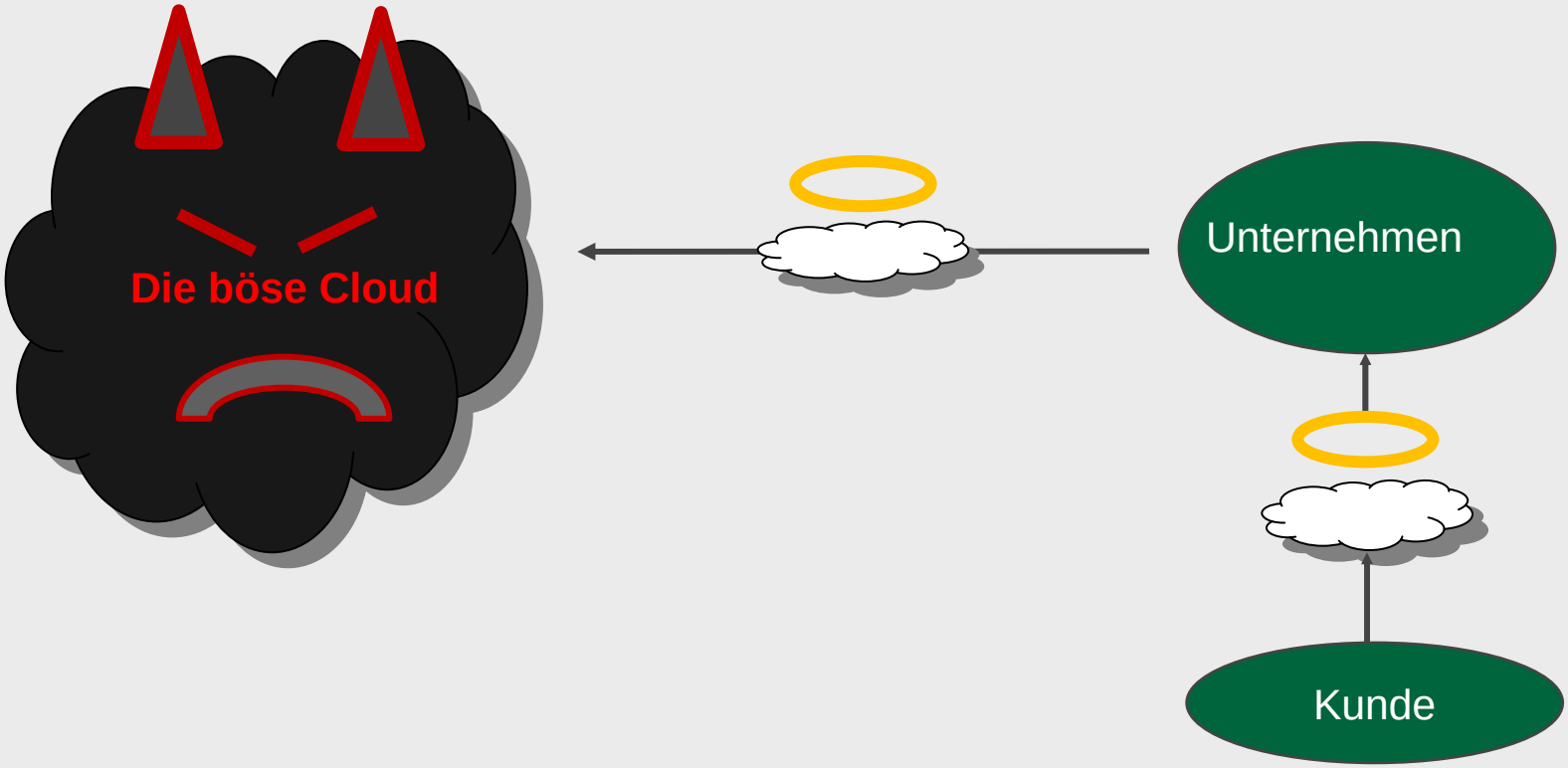
Beschäftigtendatenschutz

- Information:
  - Transparenz der Information, Zweckbindung
- Mitbestimmung:
- 87 I Nr. 6 BetrVG
- Einwilligung:
  - Einwilligung im Arbeitsverhältnis möglich
- Art. 88 EU-DSGVO: Nationale Regelungen möglich

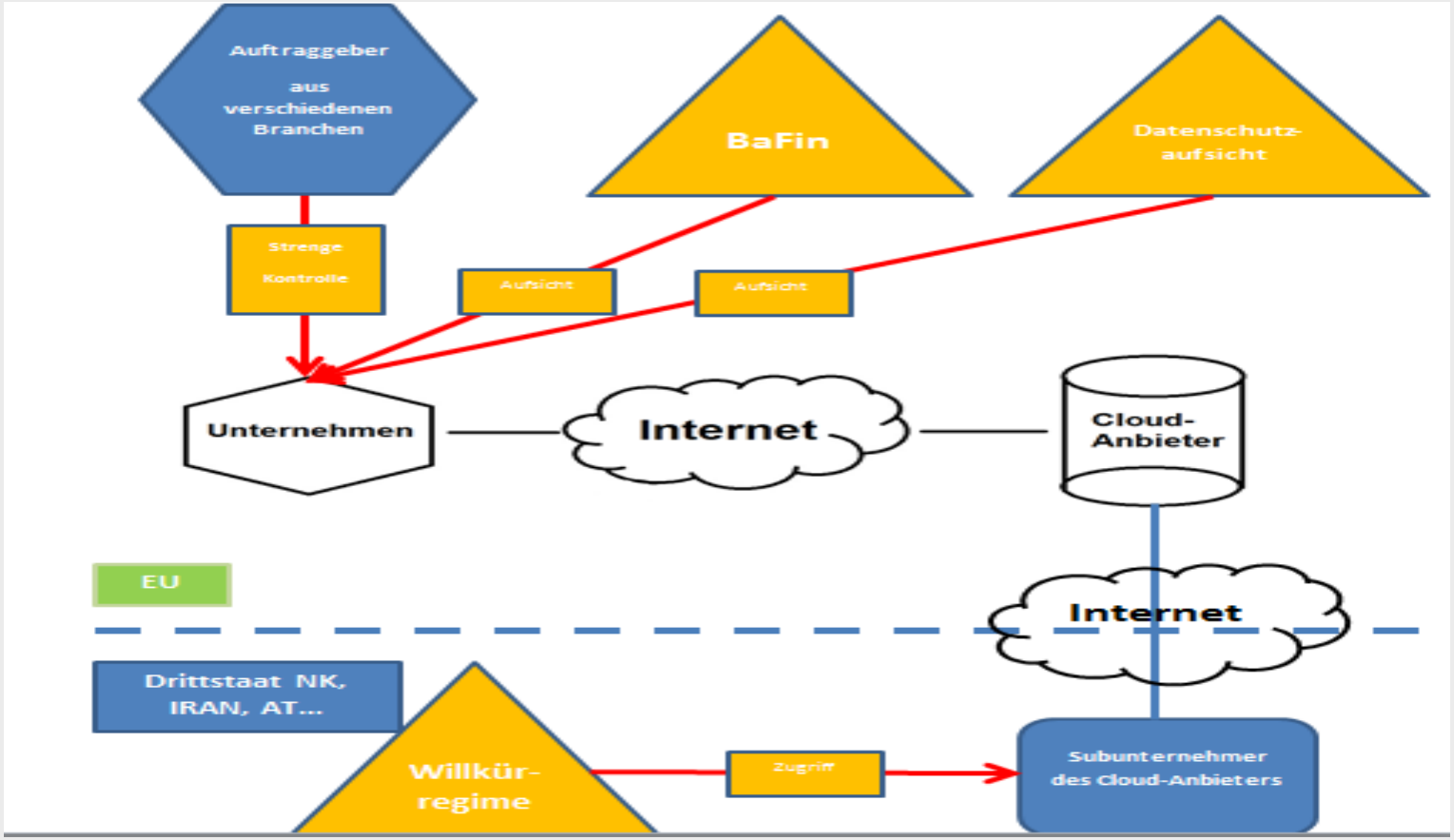
Cloud Computing: Was ist das?



Cloud Computing: Wo ist denn die Cloud?



Cloud Computing: Probleme?



Grundfragen

- Wie sensibel sind die Daten?
- Wer ist „verantwortliche Stelle“?
- Findet deutsches Recht Anwendung?
- Welche Datennutzung findet statt?
- Welche Datenübertragung ist problematisch?
- Was sind mögliche Verletzungsfolgen?

Cloud Computing: Datenarten im Detail

Wie sensibel sind die Daten?

- „Besondere Arten personenbezogener Daten" gemäß § 3 Abs. 9 BDSG wie Gesundheitsdaten, Sozialdaten oder besondere Berufs- und Dienstgeheimnisse gemäß § 80 SGB X und gemäß § 203 StGB für Ärzte, Versicherungen, Anwälte, Steuerberater, Wirtschaftsprüfer und andere
- Beschäftigten- oder Personaldaten gemäß BetrVG
- Kundendaten gemäß vertraglichen Vorgaben und Vorgaben des Fernabsatzrechts gemäß § 312b BGB
- Daten, die dem Fernmeldegeheimnis unterliegen (§ 88 TKG), und Telekommunikationsdaten im Sinne der §§ 91 ff. TKG
- Im Rahmen eines Telemedienangebots erhobene Daten gemäß §§ 13 TMG (Telemediengesetz)
- Daten über Finanzgeschäfte gemäß § 25a KWG sowie nach den Bestimmungen des GwG
- Verbraucherdaten oder archivierungspflichtige Daten nach § 257 HGB und § 146 AO

Cloud Computing: Empfehlungen

- Einordnung
  - Kombination aus Auslandsdatenübertragung und Transfer an Dritte
  - Komplexe Verantwortungsregelung
  - Risiko des Zugriffsverlusts
- Besondere Herausforderungen:
  - Besondere Personenbezogene Daten
  - Geheimnisschutz 203 StGB
  - Betriebs- und Geschäftsgeheimnisse
  - Know-How
  - NDA-Daten

Cloud Computing: Empfehlungen

ADV / FÜ / GV / Datentransfer
Vertragsinhalte

- Passende Vorgaben machen:
- DSDS, Anlage zu § 9 BDSG
- Meldeverpflichtung nach § 42a BDSG
- Referenzen
- Physikalische Datentrennungen
- Zugriffsschutz
- Subunternehmerausschluss
- Standorte regeln (kein GB, VS etc.)
- Zertifikate beachten / VeriMetrix

Der ausgerufene Patient...

Beispiel Patientendaten

Umgang mit Daten

§ 3a Datenvermeidung und Datensparsamkeit

Beispiel im Gesundheitsbereich:

Die Apothekenkasse...

Die Auskunft im Krankenhaus

Beispiel Patientendaten

https://www.test.de/Datenschutz-beim-Arzt-Laxer-Umgang-mit-Patientendaten-4980163-0/
18.03.2016
„Datenlecks in jedem zweiten Fall

Bei der Hälfte der Praxen stießen wir auf Verstöße gegen Daten-schutz-regeln, teils leichte, teils sogar drastische. Bei acht von zehn Anrufen gaben Mitarbeiter Vertrauliches über die Testpatienten preis, etwa Labor-werte oder verordnete Arzneien – ohne die Berechtigung der Anrufer zu hinterfragen. Das erleichtert es Unbe-fugten, unter einem Vorwand Informationen abzugreifen – wie im Eingangs-beispiel.
Ebenfalls bedenk-lich: der sorglose Umgang mit Patienten-E-Mails. Bei vier unserer Anfragen schickten Praxis-mit-arbeiter Infos unver-schlüsselt an Adressen, die nun wirk-lich von jedermann stammen könnten, wie sommer-wind_x@gmx.de.“

http://www.morgenpost.de/berlin/article207275825/Patientendaten-Sicherheitsluecken-bei-der-Charite.html

Zugang zum Krankenhausnetzwerk über Erfassungsnotebooks
(Details JB 2015 https://datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte)

8. Beispiel Patientendaten

Rechtsgrundlagen

- *BDSG*
- *LDSG*
- *LKHG*
- *SGB V*
- *Medizinisches Standesrecht*
- *Strafrecht*

- *Spezialgesetze*
  - *TransplantationsG*
  - *RöntgenVO*
  - *Etc*
  - *GDG*
  - *Patuientenrechtegesetz*
- *Patiententenvertrag*
- *GoA (Notfälle)*

8. Beispiel Patientendaten

*§ 9 MBO-Ä (2015) ärztliche **Schweigepflicht.***

(1) Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist - auch über den Tod des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.
(2) Der Arzt ist zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutz eines höherrangiges Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht des Arztes einschränken, soll der Arzt den Patienten darüber unterrichten.
(3) Der Arzt hat seine Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.
(4) Wenn mehrere Ärzte gleichzeitig oder nacheinander den selben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist.

8. Beispiel Patientendaten

***§ 203 StGB** Verletzung von Privatgeheimnissen*

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis ... offenbart, das ihm
1. als Arzt, Zahnarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatliche Ausbildung erfordert, ...
anvertraut worden oder sonstwie bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. ...
(3) Den in Absatz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlass erlangt hat.
(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

Beispiel Patientendaten

Hinweise der Aufsichtsbehörden u.a.:

Patientendatenschutz im Krankenhaus (ULD)
https://www.datenschutzzentrum.de/medizin/krankenh/patdskh.htm

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen
https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/050502011Krankenhausinformationssysteme.pdf?__blob=publicationFile

Beispiel Patientendaten

"Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz)"

Fahrplan zur digitalen Vernetzung für die Selbstverwaltung und für die weiteren Schritte mit nutzbringenden Anwendungen.

Patienten erhalten ab 2018 einen Anspruch darauf, dass ihre auf der Gesundheitskarte gespeicherten Daten in ein elektronisches Patientenfach aufgenommen werden.

Beispiel Patientendaten

Typische Probleme

- *Wann sind Patientendaten „erforderlich“? Dr. House – Problem!*
- *Kollision Dokumentationspflichten / Datenlöschungspflichten*
- *Patientennamen auf Stationen*
- *Ist das Einstellen in ein konzernweites "Intranet„ eine Datenweitergabe?*
- *Datenweitergabe an andere Ärzte, Krankenhäuser, Labore….*
- *Weitergabe Daten aus MVZs?*

Beispiel Patientendaten

Berliner TB 2015

„Wer den eigenen Patientinnen und Patienten diese Kommunikationsformen eröffnen will, muss die Voraussetzungen dafür schaffen, dass die Vertraulichkeit gewahrt bleibt. In der Regel wird dabei ein Dienstleister einbezogen. Dies muss für die Betroffenen transparent sein. Da der Dienstleister in der Regel zumindest Kenntnis von dem Bestehen des Behandlungsverhältnisses erhält, ist eine ausdrückliche Schweigepflichtentbindung durch die Betroffenen notwendig.“

„Nichts anders gilt für die Übertragung von einem mobilen Gerät aus, das die Betroffenen bei sich tragen, sei es, dass sie eine App auf ihrem Smartphone nutzen, um den Fortschritt der Therapie zu dokumentieren, sei es, dass ein am Körper getragenes Messgerät über die Mobilfunkverbindung Daten kontinuierlich überträgt. In dieser Konstellation dürfen die empfangenden Server nicht „irgendwo in der Cloud“, sondern ausschließlich bei dem vereinbarten Dienstleister landen, der sie dann an die jeweilig behandelnde Person überträgt. Verschlüsselung und gegenseitige Authentisierung bei allen Verbindungen sind Pflicht.“

Beispiel Patientendaten

http://www.pwc.de/de/pressemitteilungen/2016/patienten-fuerchten-datenmissbrauch-im-gesundheitswesen.html

Frankfurt, 11. April 2016

„Nur 22 Prozent der gesetzlich Versicherten und 14 Prozent der Privatversicherten begrüßen dieses Gesetz [e-health-Gesetz] ohne Einschränkung, 47 Prozent der Privatversicherten und 43 Prozent der gesetzlich Versicherten sind jedoch nach wie vor misstrauisch.“

Verletzungsfolgen, Maßnahmen der Datenschutzaufsicht

a) Behördliche Maßnahmen (Ordnungswidrigkeiten u. Strafrecht)

- Bußgeld bis zu 300.000,00 EUR, § 43 BDSG
- Höhere Bußgelder nach §§ 30, 130 OWiG (z.B. 1,3 Mio. EUR, „Debeka-Fall“)
- Freiheitsstrafe bis zu 2 Jahren, § 44 BDSG
- **Neu ab 2018:** bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens oder (für andere Datenverarbeiter) bis zu 20 Mio. EUR, Art. 83 EU DSGVO
- Persönliche Haftung
- Sonstige Maßnahmen der Aufsichtsbehörden

Verletzungsfolgen, Maßnahmen der Datenschutzaufsicht

b) Zivilrechtliche Ansprüche

- Unterlassung
- Auskunft
- Schadensersatz
- Betroffeneninformation
- Persönliche Haftung
- **Neu seit 24.02.2016:** Verbandsklagerecht (Unterlassungsklagen von Verbraucherverbänden gegen Unternehmen, wenn diese gegen Datenschutzrecht verstoßen und so Verbraucherrechte verletzen),

  Aber: Aussetzung d. Klagemöglichkeit bis 30.09.2016, soweit Datenübermittlungen auf Basis von Safe Harbor stattgefunden haben

avocado
rechtsanwälte

Prof. Dr. Thomas Wilmer, Counsel

Standort: Frankfurt

Schwerpunkte:
IT- und IP-Recht, E-Commerce, Datenschutz, Compliance

Sprachen: Deutsch, Englisch

Mitgliedschaften:
Deutsche Gesellschaft für Recht und Informatik,
Deutsch-Brasilianische Juristen-vereinigung,
Internationaler Arbeitskreis Contract Management

Kontakt:
t +49 [0]69.91 33 01 1392
f +49 [0]69.91 33 01 120
wilmer@avocado.de

CV, Expertise:

•seit 1994 Beratung im IT-Vertriebsrecht, IT-Einkauf, IP Due Diligence sowie Datenschutzrecht, langjährige Erfahrung sowohl bei der internationalen Anbieter- als auch der Anwenderberatung (juristische, kaufmännische und technische Fragestellungen)

•seit 2002 Professor für Informationsrecht an der Hochschule Darmstadt

•betrieblicher Datenschutzbeauftragter der Hochschule Darmstadt und weiterer Mandanten von avocado rechtsanwälte

•seit 2004 Geschäftsführender Direktor des Instituts für Informationsrecht und seit 2006 Dozent der „Fachanwaltsausbildung für Informationstechnologie“

•seit 2010 Leitung des Studiengangs „Internationales Lizenzrecht“ LL.M.

•seit 2010 Counsel bei avocado rechtsanwälte

•Publikationen zum Informations- und Datenschutzrecht, Referent bei Inhouse-Fortbildungen

Danke für Ihre Aufmerksamkeit!

...und wenn Sie an weiteren Neuigkeiten interessiert sind:

avocado rechtsanwälte
Schillerstraße 20 60313 **frankfurt**
t +49 [0]69. 913 30 10 f +49 [0]69. 91 33 01 19
frankfurt@avocado.de
www.avocado.de