IP-Grundlagen & Datenschutz-Grundverordnung

RA Dr. Lukas Feiler, SSCP CIPP/E

10. Jänner 2018

Themen

1 Grundlagen des Urheberrechts

Wann ist ein Werk urheberrechtlich geschützt?

- Schutz setzt voraus
  - eigentümliche
  - geistige Schöpfung

  → erforderliche Eigenart ist sehr gering (zB OGH 4 Ob 179/01d – Eurobike)
- auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste, der Filmkunst.

- Registrierung nicht erforderlich (≠ Patentrecht)

Geschützt?

Geschützt?

MASCHINELLES LERNEN

Googles KI schreibt schlechte Liebesgedichte

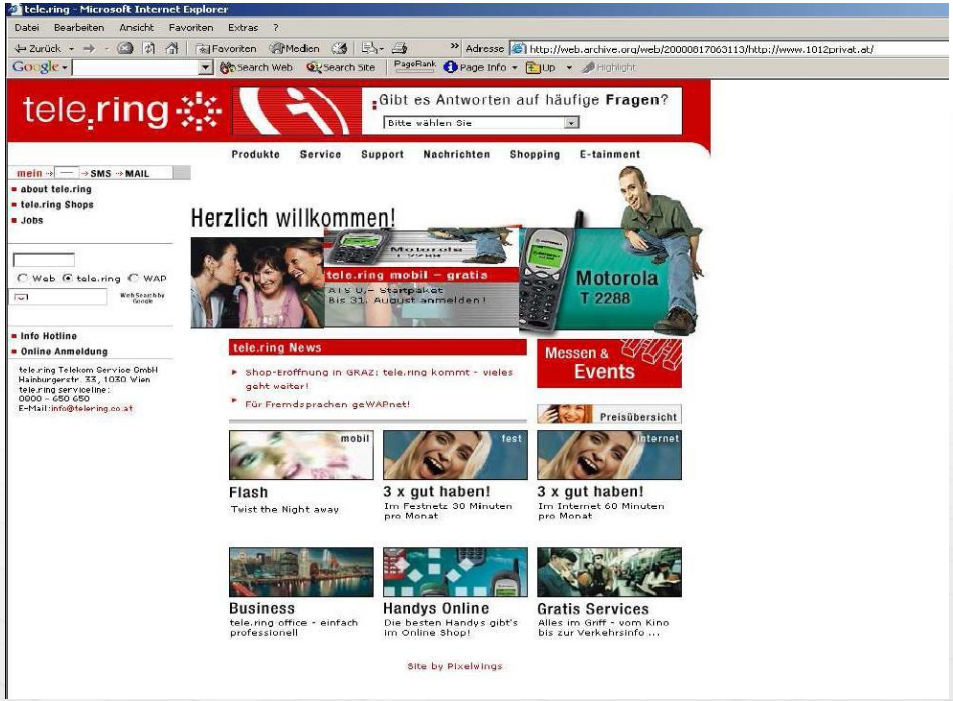
Mit maschinellem Lernen will Google sinnvolle Dialoge erzeugen. Als Trainingsdaten dienen dafür unter anderem Liebesromane. Das Ergebnis erinnert aber teils mehr an absurde Gedichte als an schmachtende Texte.

Einzelne Sätze und deren Aufbau verstehen, das können Maschinen inzwischen schon sehr gut, wie Google erst vergangene Woche mit seinem Englisch-Parser Parsey McParseface bewiesen hat. Satzübergreifend Zusammenhänge in Dialogen zu erkennen oder sinnvolle Dialoge gar selbst zu erzeugen, scheint dagegen noch extrem schwierig zu sein, was die Forschungsabteilung von Google

Die Forschungsabteilung von Google versucht sich jetzt auch an Romantik - rein wisschenschaftlich natürlich.
(Bild: flickr.com, josh.greentee/CC-BY-SA 2.0)

Datum:	17.5.2016, 17:21
Autor:	Sebastian Grüner
Themen:	Maschinelles Lernen, Bundesregierung, Deep Learning, KI, Google, Applikationen, Wissenschaft

Geschützt?



Rechte nach dem Urheberrecht

- Exklusive Verwertungsrechte
  - Vervielfältigung – auch durch Aufruf einer Website?
  - Verbreitung – Werkstücke in körperlicher Form zugänglich machen
  - Vermieten und Verleihen von Werkstücken
  - Senden – z.B. echtes Online-Radio
  - Öffentlich zur Verfügung stellen (auf individuellen Abruf)
  - Öffentlich Vortragen/Aufführen/Vorführen
  - Bearbeiten – z.B. Sicherheitlücke in einer Software patchen?

2 Grundlagen des Markenrechts

Grundlagen des Markenrechts

- Rechtserwerb erst durch Eintragung im Markenregister
- Marke kann alles sein, das sich graphisch darstellen lässt – Bildmarken – Wortbildmarken - Wortmarken

Facebook

- Herkunfts/Unterscheidungsfunktion für bestimmte Waren und Dienstleistungen
- Markeninhaber kann Dritten die Verwendung ähnlicher Zeichen für ähnliche Waren/Dienstleistungen untersagen
  - z.B. „iPad“ vs. „Mi Pad“ für Tablets
- Gültigkeitsdauer: grds unbeschränkt (vorbehaltlich Verlängerungsgebühr)

3 Die Datenschutz-Grundverordnung

3.1 Einleitung in die Datenschutz-Grundverordnung

Wozu Datenschutz-Compliance?

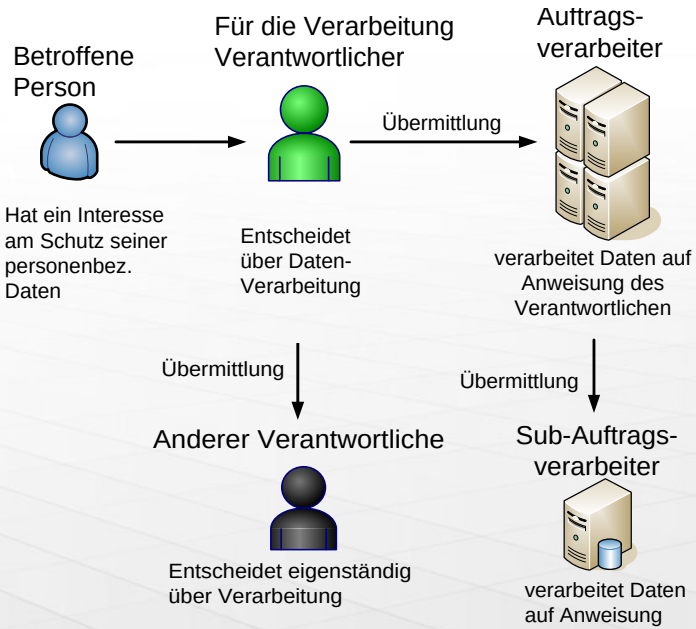
- Bisher:
  - In Österreich: Datenschutzgesetz 2000 (DSG 2000)
- Ab 25. Mai 2018: Datenschutz-Grundverordnung der EU (DSGVO)
  - Geldstrafen von bis zu 20 Millionen Euro oder vier Prozent des gesamten, weltweit erzielten Jahresumsatzes
- Haftung der Geschäftsleitung
  - Für Verwaltungsstrafen haften Mitglieder der Geschäftsleitung grds solidarisch mit der Gesellschaft
  - Haftung gegenüber der Gesellschaft aus Dienstvertrag

Anwendungsbereich

Welche Datenverarbeitungen sind erfasst?

- Jede Verarbeitung personenbezogener Daten ist erfasst
- Verarbeiten: jede Handhabung personenbezogener Daten (auch das Gespeichert-Halten)
- Personenbezogene Daten: Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen
  - DSG 2000: natürliche und juristische Personen
  - DSGVO: nur natürliche Personen

Die Rollenverteilung der DSGVO



3.2 Umsetzung der DSGVO in 12 Schritten

Schritt 1

Unterstützung aus dem Management sichern

DSGVO-Umsetzung erfordert

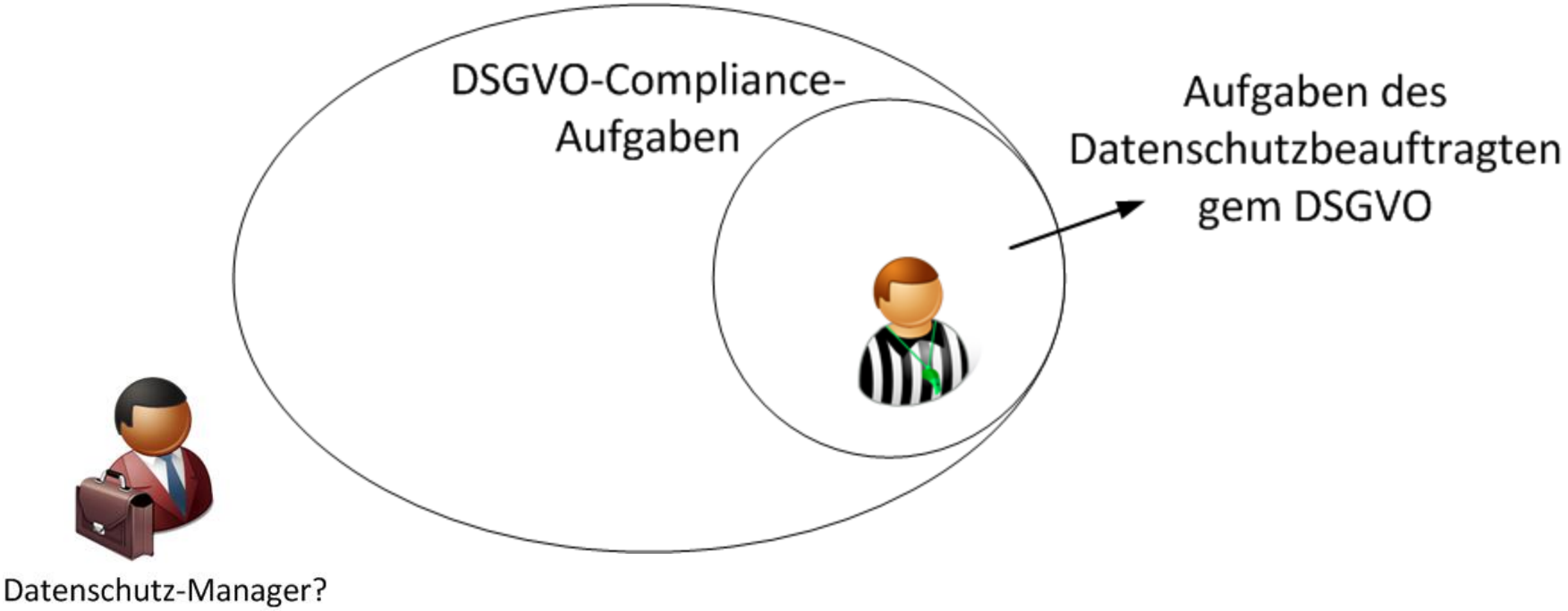
- Personalressourcen
- Budget
- (unternehmens-)politische Unterstützung

Motivation des Managements?

- persönliche Haftung (im Regress) für Verstöße
- negative PR und Verlust der Mangementposition

Schritt 2

Datenschutzbeauftragten/Manager ernennen



Schritt 3

Ersten Überblick verschaffen

Welche Arten von IT-Systemen nutzt das Unternehmen?

- Mitarbeiterdaten: Lohnbuchhaltung, E-Mail-System, Telefonsystem, Personalinformationssystem, …
- Kundendaten: Rechnungswesen, CRM-System, Lohnbuchhaltung, …
- Lieferantendaten: Rechnungswesen, …

Wie sieht die gesellschaftsrechtliche Struktur des Unternehmens aus?

- Welche Gesellschaften/Niederlassungen in welchen Ländern?
- Beteiligungsstrukturen?

Welche Geschäftssparten hat das Unternehmen?

- B2B und/oder B2C

Schritt 4

Ziele des Datenschutzmanagements definieren

Konzernweite Datenschutzstrategie vs. dezentraler Ansatz

- Für welche Gesellschaften ist die Datenschutzstrategie verbindlich?

Aus personenbezogenen Daten einen wirtschaftlicher Wert gewinnen?

- Defensive vs. offensive Datenschutzstrategie

100% Compliance oder pragmatischer Compliance-Ansatz?

- Betriebswirtschaftliche vs. politische Risiken

Wer ist wofür zuständig?

- Rollen und Verantwortlichkeiten definieren

Schritt 5

IT-Tools für Datenschutz-Management auswählen

Richtige Werkzeuge erleichtern die Arbeit – MS Office-Vorlagen vs. Online-Tools:

- Verzeichnis der Verarbeitungstätigkeiten
- Privacy Impact Assessments
- Verzeichnis der Sicherheitsverletzungen

Schritt 6

Infos über Datenverarbeitungsprozesse erheben

Für jede Verarbeitungstätigkeit zu klären:

- Wer ist der Verantwortliche?
- Welche Datenkategorien werden verarbeitet?
- Zu welchen Zwecken erfolgt die Verarbeitung?
- Werden Auftragsverarbeiter eingesetzt? (Welche? Wo? Vertragsgrundlage?)
- Werden Daten an andere Verantwortliche übermittelt? (Welche? An wen? Zu welchen Zwecken? Wohin? Vertragsgrundlage?)
- Verarbeitung auf Grundlage einer Einwilligung? (Kopie der Einwilligungserklärung?)
- Kopie der Datenschutzmitteilung (sofern vorhanden)
- Datensicherheitsmaßnahmen

→ Vorbedingung für VZ der Verarbeitungstätigkeiten (Schritt 7) und Prüfung der Rechtsmäßigkeit (Schritt 8)

Schritt 7

Verzeichnis der Verarbeitungstätigkeiten erstellen

Informationen aus Schritt 6 mit Tools aus Schritt 5 erfassen

Ausnahme von der Pflicht zur Führung eines Verzeichnisses

- weniger als 250 Mitarbeiter *und*
- Verarbeitung birgt keine Risiken für Betroffene *und*
- Verarbeitung erfolgt nur gelegentlich *und*
- Verarbeitung umfasst keine sensiblen oder strafrechtlich relevanten Daten.

Schritt 8

Rechtmäßigkeit der Verarbeitungstätigen prüfen

Für jede Verarbeitungstätigkeit

- Rechtsgrundlage für Datenverarbeitung identifizieren
- ggfls. wirksame Zustimmungserklärungen entwerfen
- Datenschutzmitteilungen korrekt gestalten
- Auftragsdatenverarbeitungsvereinbarungen mit Dienstleistern abschließen
- Wo erforderlich Standardvertragsklauseln für internationale Datenübermittlungen vereinbaren

Schritt 9

Privacy Impact Assessments durchführen

Für jede Verarbeitungstätigkeit

- Prüfen, ob prima facie ein hohes Risiko für Betroffene gegeben ist (z.B. sensible Daten, Profiling oder „schwarze Liste“ der Datenschutzbehörde)
  - Grds kein hohes Risiko, „wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt“ (Erwägungsgrund 91 DSGVO)
- Nur wenn prima facie hohes Risiko gegeben ist: Privacy Impact Assessment durchführen
- Wenn PIA ein hohes Risiko ergibt: Konsultation mit der Datenschutzbehörde

Schritt 10

Datenschutzrelevante Unternehmensrichtlinien

Datenschutzrelevante Unternehmensrichtlinien erstellen

- Richtlinie zum Umgang mit personenbezogenen Daten
- Richtlinie zur Informationssicherheit
- Richtlinie zur Reaktion auf Zwischenfälle
- Richtlinie zur Nutzung der Unternehmens-IT
- BYOD-Richtlinie
- …

Schritt 11

Konzept für Info-Maßnahmen und Schulungen

Konzept für unternehmensinterne Informationsmaßnahmen und Schulungen erstellen

- Wen wie oft schulen?
- Kreatives Awareness-Raising
- Compliance am Papier vs. tatsächliche Compliance

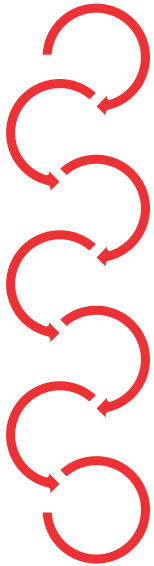
Schritt 12

Datenschutz im täglichen Betrieb aufrechterhalten

DSGVO-Umsetzung kontinuierliche Compliance-Maßnahmen:

- Audits durchführen
- Schulungen abhalten
- Auf Zwischenfälle reagieren
- Anfragen von Betroffenen bearbeiten
- Neue Verarbeitungstätigkeiten erfassen
- An das Management berichten

Schritte 1 bis 12
Übersicht



1) Unterstützung aus dem Management sichern
2) Datenschutzbeauftragten/Manager ernennen
3) Ersten Überblick verschaffen
4) Ziele des Datenschutzmanagements definieren
5) IT-Tools für das Datenschutz-Management auswählen
6) Informationen über Datenverarbeitungsprozesse erheben
7) Verzeichnis der Verarbeitungstätigkeiten erstellen
8) Rechtmäßigkeit der Verarbeitungstätigen prüfen
9) Datenschutz-Folgeabschätzungen durchführen
10) Datenschutzrelevante Unternehmensrichtlinien erstellen
11) Konzept für Informationsmaßnahmen & Schulungen
12) Datenschutz im täglichen Betrieb aufrechterhalten

3.3 Einzelheiten zu den Pflichten nach der DSGVO

Verhältnis zu nationalem Recht

Rechtsdurchsetzung durch nationale Behörden

- Durchsetzung durch die nationalen Aufsichtsbehörden
  - Europäische Kommission hat keine Durchsetzungsbefugnis
  - Europäischer Datenschutzausschuss
    - Ersetzt Artikel-29-Datenschutzgruppe
    - Nur zuständig für Streitigkeiten zwischen Aufsichtsbehörden

Grundsätze der Datenverarbeitung

- Rechtmäßigkeit (Rechtsgrundlage für Verarbeitung erforderlich)
- Treu und Glauben
- Transparenz
- Zweckfestlegung
- Zweckbindung
- Richtigkeit
- Datenminimierung
- Speicherbegrenzung
- Sicherheit
- Rechenschaftspflicht

Rechtmäßigkeit der Datenverarbeitung

Datenschutzrechtliche Rechtsgrundlagen

1. Einwilligung der betroffenen Person (informierte und freiwillige Zustimmung)
2. Erforderlichkeit für die Erfüllung des mit betroffener Person geschlossenen Vertrages
3. Gesetzliche Verpflichtung des Verantwortlichen
4. Lebenswichtige Interessen der betroffenen Person
5. Erforderlichkeit für Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt
6. Überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten

Rechtmäßigkeit der Datenverarbeitung

Neue Grenzen für die elektronische Einwilligung

- Schlüssige oder ausdrückliche Zustimmung
- Checkbox darf nicht per Default angehakt sein
- Zustimmung durch AGB?
  - in verständlicher und leicht zugänglicher Form
  - in klarer und einfacher Sprache
  - von anderen Regelungsgegenständen der AGB klar zu unterscheiden

Rechtmäßigkeit der Datenverarbeitung

Einwilligung von Personen unter 16 Jahren

- Zustimmung von Minderjährigen für Online-Dienste grds erst gültig ab 16 Jahren
- < 16 Jahre: Zustimmung der Erziehungsberechtigten erforderlich
  - Verantwortlicher muss „angemessene Anstrengungen unter Berücksichtigung der vorhandenen Technologie“ unternehmen
- Praktische Umsetzung
  - Angebot nicht auf Unter-16-Jährige ausrichten
  - Registrierung nur zulassen, wenn Geburtsdatum angegeben
- Nationales Recht: Altersgrenze kann auf bis zu 13 Jahre herabgesetzt werden

Rechtmäßigkeit der Datenverarbeitung

Herausforderung für Gratis-Dienste

- Viele „Gratis“-Dienste im Internet setzen Zustimmung zur Datenerhebung voraus
- Zustimmung nur gültig, wenn sie „frei“ ist
- Grds nicht „frei“, wenn

die Durchführung eines Vertrages von Zustimmung zur Datenverarbeitung abhängig gemacht wird und

  - die Datenverarbeitung für die Vertragserfüllung nicht erforderlich ist

- Stehen die datengestützten Geschäftsmodelle auf dem Spiel?
  - Die Einwilligung kann für die Vertragserfüllung (wirtschaftlich) notwendig sein
  - Alternativ anbieten:
    - keine Gebühr + datenschutzrechtliche Einwilligung oder
    - angemessene Gebühr

Rechtmäßigkeit der Datenverarbeitung

Einwilligung bei sensiblen Daten

- Als sensible Daten gelten: Daten aus denen
  - rassische und ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder weltanschauliche Überzeugungen oder
  - Gewerkschaftszugehörigkeit hervorgeht

  und
  - genetische und biometrische Daten zur Identifizierung einer natürlichen Person
  - Gesundheitsdaten sowie Daten zum Sexualleben

→ überwiegendes berechtigtes Interesse ist nicht ausreichend

→ Einwilligung muss ausdrücklich erfolgen

Der Datenschutzbeauftragte

Bestellung

- DSG 2000: Keine Regelungen
- Mit der DSGVO verpflichtend, wenn
  - Verarbeitung durch Behörde oder öffentliche Stelle

    oder
  - Daten-getriebenes Geschäftsmodell
    - Kerntätigkeit des Unternehmens ist umfangreiche regelmäßige und systematische Überwachung von Betroffenen
    - Kerntätigkeit des Unternehmens ist die umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten

    oder
  - nach nationalem Recht vorgeschrieben (voraussichtlich nicht in Österreich)

Persönliche Voraussetzungen

- Persönliche Voraussetzungen
  - berufliche Qualifikation und Fachwissen auf dem Gebiet des Datenschutzrechts
  - kann, muss aber nicht Arbeitnehmer des Verantwortlichen sein
  - es darf kein Interessenskonflikt vorliegen
- Bestellung eines externen Datenschutzbeauftragten ist möglich

Der Datenschutzbeauftragte

Stellung im Unternehmen

- weisungsfrei
- genießt Kündigungsschutz
- unmittelbare Berichterstattung an die höchste Managementebene
- Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen
- muss über alle notwendigen Ressourcen verfügen
- hat Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
- Anlaufstelle für betroffene Personen
- Verschwiegenheitsverpflichtung
- Grds keine Haftung nach der DSGVO

Outsourcing an Auftragsverarbeiter

- Verantwortlicher kann sich zur Datenverarbeitung eines Auftragsverarbeiters bedienen
  - Auftragsverarbeiter muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten
- Auftragsverarbeitervereinbarung muss Pflichten des Auftragsverarbeiters festlegen:
  - Verarbeitung nur auf dokumentierte Weisungen des Verantwortlichen;
  - Vertraulichkeit von zur Verarbeitung befugter Personen gewährleisten;
  - muss notwendige Sicherheitsmaßnahmen umsetzen;
  - nach Abschluss der Leistungserbringung personenbezogene Daten löschen/zurückgeben;
  - Einsatz von Sub-Auftragsverarbeitern nur mit Genehmigung des Verantwortlichen;
  - Duldung und Unterstützung von Audits;
  - stellt dem Verantwortlichen sämtliche Informationen zum Nachweis der Einhaltung zur Verfügung

Internationale Datenübermittlungen

- Unproblematisch bei Empfängern
  - in der EU oder dem EWR;
  - in einem Drittland mit adäquatem Datenschutzniveau
    - z.B. Kanada, Schweiz
    - U.S.-Privacy-Shield: angemessener Datenschutz, wenn sich der Empfänger nach Privacy Shield selbst-zertifiziert hat
- Wenn in Drittland kein adäquates Datenschutzniveau
  - grundsätzlich „Standardvertragsklauseln“ erforderlich
    - DSG 2000: genehmigungspflichtig
    - DSGVO: keine Genehmigung erforderlich
  - Ausnahme: Einwilligung der Betroffenen

Datensicherheitspflichten

Vertraulichkeit, Verfügbarkeit, Integrität

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, des Umfangs, der Umstände & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Datensicherheitspflichten

Sicherheitsmaßnahmen

- Angemessene Maßnahmen umfassen laut DSGVO insb.:
  - Pseudonymisierung und Verschlüsselung;
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, die Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. „Critical Security Controls for Effective Cyber Defense“ des Center for Internet Security (CIS) oder ISO/IEC 27001

Typen von Sicherheitsmaßnahmen

- Nach der Art der Maßnahme: Technische, organisatorische und physische Maßnahmen
- Nach der Wirkungsweise: präventive, detektive, reaktive oder absreckende Maßnahmen

Beispiele	Technical	Organizational	Physical
Präventiv	Firewall	4-Augen-Prinzip	Stahltür
Detektiv	Intrusion Detection System	Verpflichtender Log Review	Brandmelder
Reaktiv	(Backup &) Restore	Incident Response Policy	Feueralarm
Abschreckend	Warnmeldung	Disziplinarordnung	Hund

Melde- und Dokumentationspflichten

Meldung von Datensicherheitsverstößen

- auch Pflicht zur „Data Breach Notification“
- Eine Verletzung des Schutzes personenbezogener Daten muss der Aufsichtsbehörde unverzüglich und spätestens binnen 72 Stunden gemeldet werden
- Pflicht zur Notifikation gegenüber betroffenen Personen nur, wenn das bestehende Risiko hoch ist

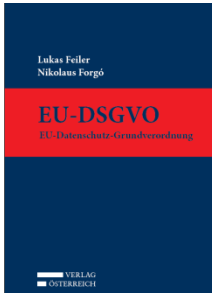
Verhängung und Bemessung von Geldstrafen

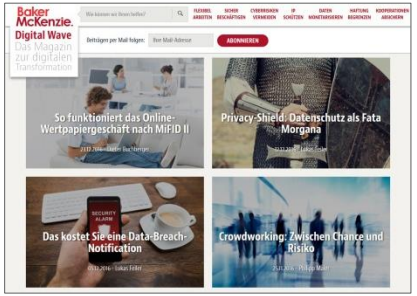
- Strafrahmen nach DSGVO: bis zu 20 Millionen Euro oder vier Prozent des weltweiten, jährlichen Umsatzes des Unternehmens
- Unionskartellrechtlicher Unternehmensbegriff
  - Bemessung der Strafe: weltweiter Umsatz des gesamten Konzerns maßgeblich
  - Strafe kann auch über Konzernmutter verhängt werden
    - Mitverantwortung der Konzernobergesellschaft, wenn Tochtergesellschaft Verhalten nicht autonom bestimmt
    - widerlegliche Vermutung bei 100%-igen Tochtergesellschaften (EuGH C-107/82 – AEG)

Private Rechtsdurchsetzung

- Betroffene Person kann klagen,
  - wo sie ihren Wohnsitz hat;
  - wo der Verantwortliche/Auftragsverarbeiter eine Niederlassung hat
- Mögliche Ansprüche:
  - Betroffenenrechte (Auskunft, Löschung, …)
  - Materieller und immaterieller Schadenersatz
- Rechtsdurchsetzung durch NGOs:
  - NGOs können im Namen von Betroffenen klagen
  - Schadenersatzansprüche nur, wenn nach nationalem Recht zugelassen (nach welchem?)
  - Betroffenenrechte unabhängig von Auftrag eines Betroffenen einklagen (je nach Gerichtsstand)

Baker McKenzie.





Dr. Lukas Feiler, SSCP CIPP/E
Senior Associate
Leiter des Teams für IT-Recht in Wien

Schottenring 25
1010 Vienna

T: +43 1 24 250
lukas.feiler@bakermckenzie.com

Lukas Feiler ist Co-Autor des eines Kommentars zur Datenschutz-Grundverordnung und des ersten Praktiker-Buches zur DSGVO sowie Herausgeber des Gesetzbuch Datenschutzrecht. Er begleitet Unternehmen auf www.digitalwave.at bei der digitalen Transformation.

www.bakermckenzie.com