TAGUNGSPROGRAMM

DONNERSTAG, 23. Mai 2019

9:00-9:15 **Begrüßung** durch Univ. Prof. Dr. Andreas Wiebe, LL.M., Obmann des Forschungsvereins Infolaw

I. CYBERSECURITY UND REGULIERUNGSFRAGEN

Moderation: Dr. Roman Heidinger, MA, Forschungsverein Infolaw / Universität Göttingen

09:15-10:00 **NIS-Richtlinie und ihre Umsetzung in Österreich**
Mag. Vinzenz Heußler, Bundeskanzleramt
Ing.in Mag.a Sylvia Mayer MA, Bundesministerium für Inneres, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

10:00-10:45 **Rechtliche Rahmenbedingungen der Cybersecurity**
RA Mag. Armin Hendrich MBA MSc, DLA Piper Weiss-Tessbach

10:45-11:15 **Kaffeepause**

11:15-12:00 **E-Evidence VO**
RA Dr. Lukas Feiler SSCP, CIPP/E, Baker McKenzie

12:00-12:45 **AI als Erfinder**
PA Dr. Fabian Stanke, SONN & PARTNER Patentanwälte

12:45-13:45 **Business Lunch**

13:45-14:30 **Initial Coin Offerings** - Technische Einführung und rechtliche Probleme
RA Dr. Thomas Kulnigg, Schönherr Rechtsanwälte

II. URHEBER- UND DATENRECHT

Moderation: Univ. Prof. Dr. Andreas Wiebe, LL.M., Forschungsverein Infolaw / Universität Göttingen

14:30-15:15 **Zahlen mit Daten - vertragsrechtliche Fragen**
Dr. Andreas Sattler, LL.M., LMU München

15:15-15:45 **Kaffeepause**

16:00-16:45 **Forschung und Datenschutz - Auswirkungen des FOG**
Dr. Sebastian Reimer, Intelligent Law & Internet Applications

16:45-17:30 **Text und Data Mining aus urheber- und datenschutzrechtlicher Sicht**
Univ. Prof. Ing. Dr. Clemens Appl, LL.M., Forschungsverein Infolaw / Donau-Universität Krems

17:30-18:30 **Personenfotos aus persönlichkeits- und datenschutzrechtlicher Sicht**
RA Dr. Andreas Seling, M.B.L. und Mag. Dominik Schelling, DORDA Rechtsanwälte

19:00 **Abendempfang**

FREITAG, 24. Mai 2019

III. DATENSCHUTZ

Moderation: Univ. Prof. Ing. Dr. Clemens Appl, LL.M., Forschungsverein Infolaw / Donau-Universität Krems

9:00-10:30 **1 Jahr DSGVO – Erste Erfahrungen und Problembereiche**
Prof.in Dr.in Eva Souhrada-Kirchmayer, Richterin am Bundesverwaltungsgericht
Mag. Andreas Zavadil, Datenschutzbehörde
Dr.in Natalie Ségur-Cabernac, Hutchinson Drei Austria GmbH
RA Dr. Rainer Knyrim, Knyrim Trieb Rechtsanwälte, Wien

10:30-11:15 **Ausgewählte Probleme beim externen Datenschutzbeauftragten**
RA Mag. Roland Marko, LL.M., WOLF THEISS Rechtsanwälte

11:15-11:45 **Kaffeepause**

11:45-12:45 **Datenschutzrechtliche Implikationen des CLOUD Act für Europa**
RA Dr Axel Anderl, LL.M. und RA Mag. Nino Tlapak LL.M., DORDA Rechtsanwälte

12:45-13:30 **Datenschutzrechtliche Anforderungen an betriebliche Kommunikationsmittel**
RA Mag. Stefan Panic, DLA Piper Weiss-Tessbach

13:30-13:45 **Schlussworte**

13:45 **Farewell Business Lunch**

VERANSTALTUNGSORT:
Haus des Sports
Prinz-Eugen-Straße 12
(Nähe Schwarzenbergplatz)
1040 Wien
U-Bahn: U1, U2, U4 (Karlsplatz)
Straßenbahn: D

INFOLAW
WWW.INFOLAW.AT

13. ÖSTERREICHISCHER IT-RECHTSTAG

Der Österreichische IT-Rechtstag findet dieses Jahr bereits zum 13. Mal statt. Mit regelmäßig weit über 100 Teilnehmerinnen und Teilnehmern ist der IT-Rechtstag als zentrales Forum des Informationsrechts in Österreich etabliert. In bewährter Weise soll auch in diesem Jahr die Veranstaltung Gelegenheit bieten, aktuelle Fragen praxisnah aufzubereiten, zukünftige Trends zu beleuchten und die Verzahnung von IT-Recht, technischer Entwicklung und Geschäftsmodellen mit zu bedenken.
Selten war das IT-Recht so dynamisch wie heute. Die "Digitalisierung" aller Bereiche von Wirtschaft und Gesellschaft wirft neue Fragen in nahezu allen Rechtsbereichen auf, was die Themenwahl nicht einfach macht. Wie immer exzellent beraten von unserem Programmkomitee liegen die Schwerpunkte der diesjährigen Veranstaltung neben dem immer aktuellen "Dauerbrenner" Datenschutz im Bereich Cybersecurityand Datenrecht. Aber auch andere praxisrelevante Entwicklungen werden berücksichtigt (z.B. E-EvidenceVO). Neben den fachlichen Aspekten soll die Veranstaltung wieder ein österreichweites Forum zum Kennenlernen, für Austausch und Diskussion zwischen Wissenschaft und Praxis bieten.

Veranstalter:
Infolaw – Forschungsverein für Informations- und Immaterialgüterrecht
p.A. Medien und Recht
Danhausergasse 6/25
1040 Wien
Internet: www.infolaw.at
Email: office@infolaw.at
Telefax: 01/2533033 8850

Wissenschaftliche Leitung und Organisation:
Univ. Prof. Dr. Andreas Wiebe, LL.M.
Dr. Roman Heidinger, M.A.
Univ. Prof. Ing. Dr. Clemens Appl, LL.M.

PROGRAMMKOMITEE

Die Veranstaltung wird von einem Programmkomitee unterstützt, dem Kolleginnen und Kollegen aus Rechtsanwaltschaft, Wirtschaft, Verwaltung und Wissenschaft in Österreich angehören, die seit Jahren aktiv und an herausragender Stelle im Bereich der Informationswirtschaft und des IT-Rechts tätig sind.

Dr. Axel Anderl, LL.M. (IT-Law) - DORDA Rechtsanwälte GmbH

Univ. Prof. DDr. Walter Blocher - Leiter des Fachgebiets Bürgerliches Recht, Unternehmensrecht und Informationsrecht, Institut für Wirtschaftsrecht, Universität Kassel

Mag. René J. Bogendorfer - Geschäftsführer-Stv. der Bundessparte Information & Consulting der WKÖ

Dr. Egon Engin-Deniz - Leiter Abteilung IP und Medien, CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH

MMag. Sabine Fehringer, LL.M. - DLA Piper Weiss-Tessbach Rechtsanwälte GmbH

Dr. Georg Fellner, LL.M. - Brauneis KlauserPrändl Rechtsanwälte GmbH

Dr. DI Wolfgang Freund, LL.M. - GramaSchwaighoferVondrak Rechtsanwälte GmbH

Dr. Gregor Gessner - Hewlett Packard Enterprise

Dr. Thomas Höhne - Höhne, In der Maur & Partner Rechtsanwälte OG

Mag. Dr. Andrea Jelinek - Leiterin der Datenschutzbehörde

Dr. Rainer Knyrim - Knyrim Trieb Rechtsanwälte OG

Hon. Prof. Dr. Guido Kucsko - Schönherr Rechtsanwälte GmbH

Mag. Roland Marko, LL.M. - WOLF THEISS Rechtsanwälte GmbH

Dr. Max Mosing, LL.M. - Geistwert Rechtsanwälte

Hon. Prof. Dr. Leonhard Reis - Rechtsanwalt in Wien

Mag. Eva Sainitzer, LL.M. - Senior Director Legal ECE, Oracle Austria GmbH

Ing. Michael Schober - Der ERP Tuner e.U. und Sprecher des Ausschusses IT der Fachgruppe Unternehmensberatung und Informationstechnologie der Wirtschaftskammer Wien sowie Stv. Obmann des Fachverbandes UBIT Österreich der WKO

Dr. Maximilian Schubert, LL.M. - Generalsekretär der Internet Service Providers Austria (ISPA)

Prof. Dr. Eva Souhrada-Kirchmayer - Richterin am Bundesverwaltungsgericht

Hon. Prof. Dr. Clemens Thiele, LL.M. - EUROLAWYER® Rechtsanwälte, Salzburg

Hon. Prof. Dr. Michel Walter - Rechtsanwalt in Wien

Dr. Stephan Winklbauer, LL.M. - aringerherbstwinklbauerrechtsanwälte

Univ. Prof. Dr. Heinz Wittmann - Medien und Recht Verlags GmbH

Dr. Manfred Vogel - OGH, Senatspräsident 4. Senat

Dr. Michael Wolner, MAS - Senior Legal Counsel Litigation & Disputes EMEA, Accenture GmbH

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Die NIS-Richtlinie und ihre Umsetzung in Österreich

Mag. Vinzenz Heußler, LL.M. - Bundeskanzleramt
Ing. Mag. Sylvia Mayer - Bundesministerium für Inneres

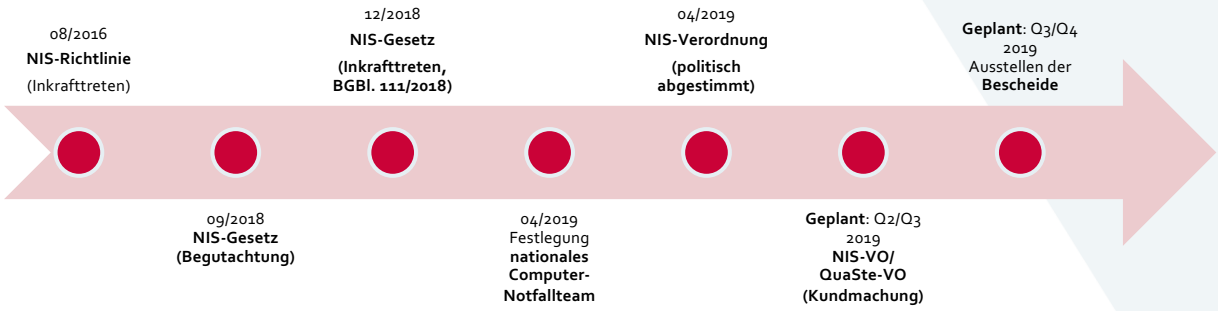
Wien, 23.05.2019

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Nationale Umsetzung der NIS-Richtlinie

Aktueller Stand



Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Anwendungsbereich (NIS-Gesetz)

"Betreiber wesentlicher Dienste"	"Anbieter digitaler Dienste"
▪ **Energie** (Elektrizität, Erdöl, Erdgas) ▪ **Verkehr** (Luft, Schiene, Straße) ▪ **Bankwesen** ▪ **Finanzmarktinfrastrukturen** ▪ **Gesundheitswesen** ▪ **Trinkwasserlieferung und -versorgung** ▪ **Digitale Infrastrukturen**	▪ **Online-Marktplatz** ▪ **Online-Suchmaschine** ▪ **Cloud-Computing-Dienst**
	Einrichtungen des Bundes
	▪ (Insbesondere) **Ministerien**

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Anwendungsbereich (NIS-Verordnung)

Wesentliche Dienste am Beispiel Energie

Elektrizität	**Stromerzeugung**	Betrieb einer Erzeugungsanlage
		Betrieb von Systemen zur Steuerung von Erzeugungsanlagen
	Stromverteilung	Betrieb eines Verteilernetzes
	Stromübertragung	Betrieb eines Übertragungsnetzes
Erdöl	**Erdölförderung**	Betrieb von Anlagen zur Förderung von Erdöl
	Erdöllagerung	Betrieb von Anlagen zur Lagerung von Erdöl
	Erdöltransport	Betrieb von Erdölfernleitungen
	Erdölraffination	Betrieb von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl
Erdgas	**Gasförderung**	Betrieb einer Gasförderungsanlagen
	Gastransport	Betrieb eines Fernleitungsnetzes
	Gasverteilung	Betrieb eines Verteilernetzes
	Gasspeicherung	Betrieb von Speicheranlagen
	...	...

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Anwendungsbereich (NIS-Verordnung)

Schwellenwerte am Beispiel Teilsektor Elektrizität

Sektor	Teilsektor	Bereich	Wesentliche Dienste	Bemessungskriterien oder Anknüpfungselemente	Schwellenwerte	Lex Specialis	Melderisiko-faktor	Materien-rechtsakte
Energie	Elektrizität	Strom-erzeugung	Betrieb einer Erzeugungsanlage	Engpassleistung in MW	xx MW	N/A	Sektoren-spezifisch	ElWOG 2010
			Betrieb von Systemen zur Steuerung von Erzeugungsanlagen	Engpassleistung in MW	xx MW	N/A	Sektoren-spezifisch	ElWOG 2010
		Strom-verteilung	Betrieb eines Verteilernetzes	Anzahl der Zählpunkte	xx	N/A	Sektoren-spezifisch	ElWOG 2010
		Strom-übertragung	Betrieb eines Übertragungsnetzes	Legalreferenz (Art der Einrichtung)	N/A	N/A	Sehr hoch	ElWOG 2010

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Zuständigkeiten

Bundeskanzler

- **Verordnungen**
  - Schwellwerte für Betreiber wesentlicher Dienste (NISV)
  - Sicherheitsvorkehrungen (NISV)
  - Kriterien für Sicherheitsvorfälle (NISV)
  - Ausnahmen von Verpflichtungen (NISV)
  - Pflichten gemeinsam datenschutzrechtlicher Verantwortlicher (NIS-PAV)
- Koordination der **Strategie**
- Koordination der **öffentlich-privaten Zusammenarbeit**
- Vertretung in **EU-Gremien**
- **Ermittlung** von **Betreibern wesentlicher Dienste** mit Bescheid
- Betrieb des **GovCERT**
- Feststellung der Eignung von **Computer-Notfallteams**

Bundesminister für Inneres

- **Verordnungen**
  - Qualifizierte Stellen (QuaSteV)
  - Ersatz für Teilnahme an IKT-Lösungen
- Betrieb einer **zentralen Anlaufstelle** (SPoC)
- Leitung der **Koordinierungsstrukturen**
- Entgegennahme/Analyse von **Meldungen**
- Erstellung eines **Lagebildes**
- Überprüfung der **Sicherheitsvorkehrungen**
- Feststellung/Überprüfung von **qualifizierten Stellen**
- Leitung des **Cyberkrisenmanagements**

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Zuständigkeiten

Koordinierungsstrukturen

Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

- Bundeskanzleramt
- Bundesministerium Inneres
- Bundesministerium Landesverteidigung
- Bundesministerium Europa, Integration und Äußeres

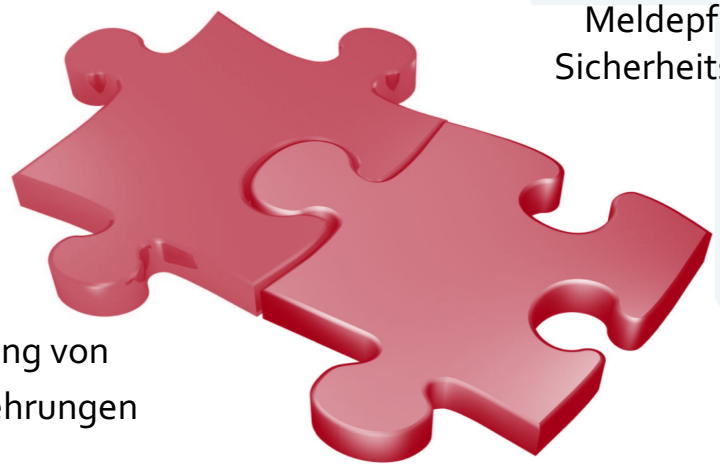
Operative Koordinierungsstruktur (OpKoord)

+ CERT.at
+ AUSTRIAN ENERGY CERT

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Verpflichtungen im Rahmen des NISG



Meldepflicht bei Sicherheitsvorfällen

Implementierung von Sicherheitsvorkehrungen

Meldung von Sicherheitsvorfällen

Definition (NISG bzw. NISV)

- ***„Sicherheitsvorfall":*** *eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat*
- „**Ausfall** des betriebenen Dienstes" die Unverfügbarkeit des Dienstes für Nutzer
- „**Einschränkung der Verfügbarkeit** des betriebenen Dienstes" die signifikant geminderte Verfügbarkeit des Dienstes in qualitativer Dimension für Nutzer

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Meldung von Sicherheitsvorfällen

Definition (NISG)

- **„Zahl der von dem Sicherheitsvorfall betroffenen Nutzer**, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen"
  - die Zahl der von einem Sicherheitsvorfall betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde,
  - oder die Zahl der betroffenen Nutzer, die den Dienst im Zeitpunkt des Sicherheitsvorfalls genutzt haben oder für die voraussichtliche Dauer des Sicherheitsvorfalls nutzen würden

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Meldung von Sicherheitsvorfällen

Schwellenwerte (NISV)

Sektorenspezifisch		Bsp: mögliche finanzielle Auswirkung von mehr als 5 Mio € oder 0,1% des harten Kernkapitals;
Niedrig	24 Stunden	Bsp: 24-stündiger Ausfall
Mittel	12 Stunden	Bsp: Ausfall für 1.056.000 Zählpunktstunden
Hoch	6 Stunden	
Sehr hoch	3 Stunden	

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Meldung von Sicherheitsvorfällen

Schwellenwerte am Beispiel Schienenverkehr

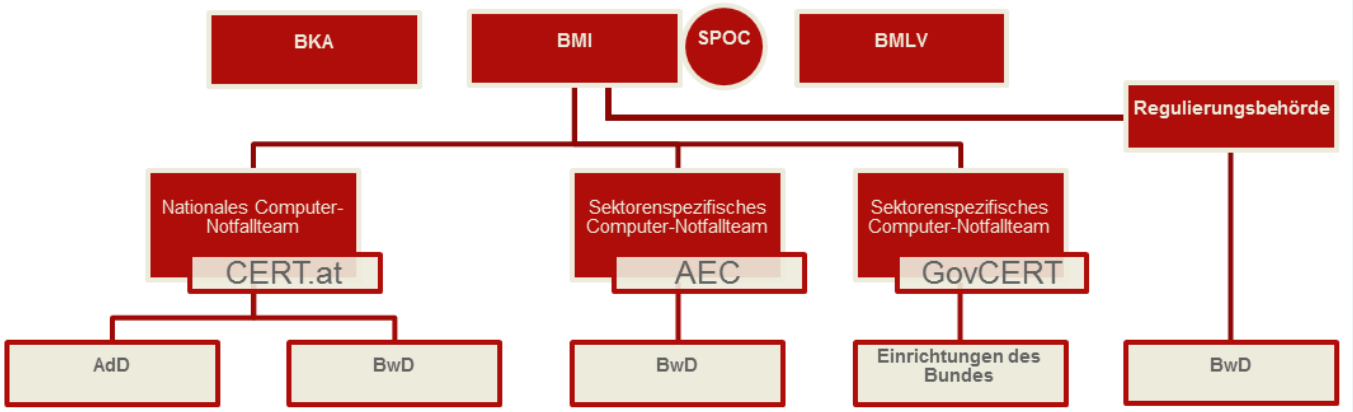
Sektor	Teil-sektor	Bereich	Wesentliche Dienste	Bemessungskriterien oder Anknüpfungselemente	Schwellen-werte	Lex Specialis	Melderisiko -faktor	Materien-rechtsakte
Verkehr	Schienen -verkehr	Infrastruktur	Betrieb von Eisenbahninfrastrukturen	Anteil an km am Kernnetz des transeuropäischen Verkehrsnetzes (TEN)	xx km	N/A	Mittel (Dauer)	EisbG und VO (EU) Nr. 1315/2013
			Betrieb von Personenhauptbahnhöfen	Landeshauptstädte	N/A	N/A	Mittel (Dauer)	N/A
		Eisenbahn-verkehrs-dienste	schienengebundene Personenbeförderung	Anzahl beförderter Passagiere pro Jahr	xx Mil.	N/A	Sehr hoch (Dauer)	N/A
			schienengebundene Beförderung von Gütern	Anzahl beförderter Tonnen Güter pro Jahr	Xx Mil.	N/A	Niedrig (Dauer)	N/A

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Meldung von Sicherheitsvorfällen

Meldewege

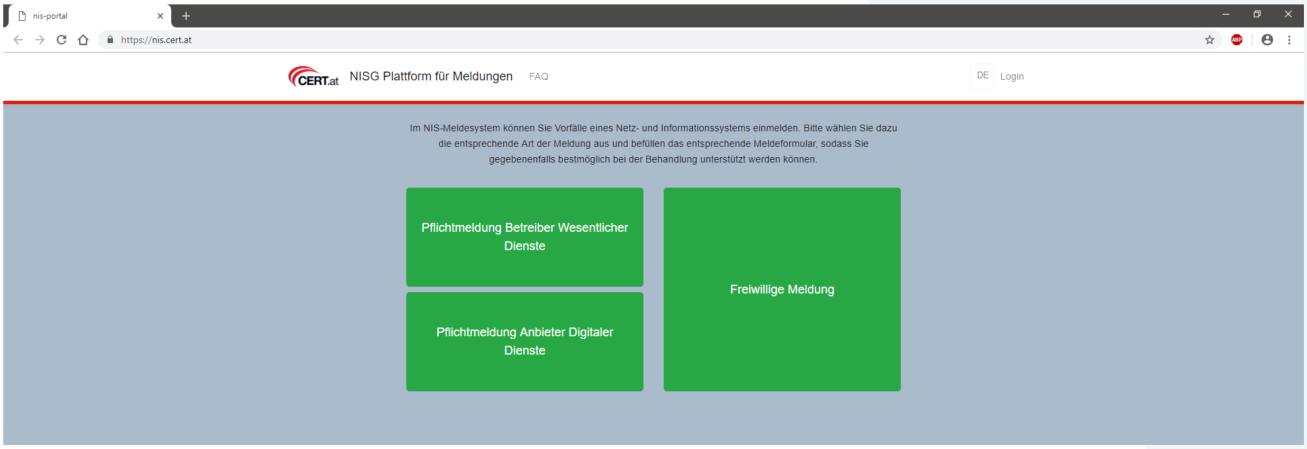


Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Meldung von Sicherheitsvorfällen

Meldeportal von CERT.at



Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

Regelungsprozess

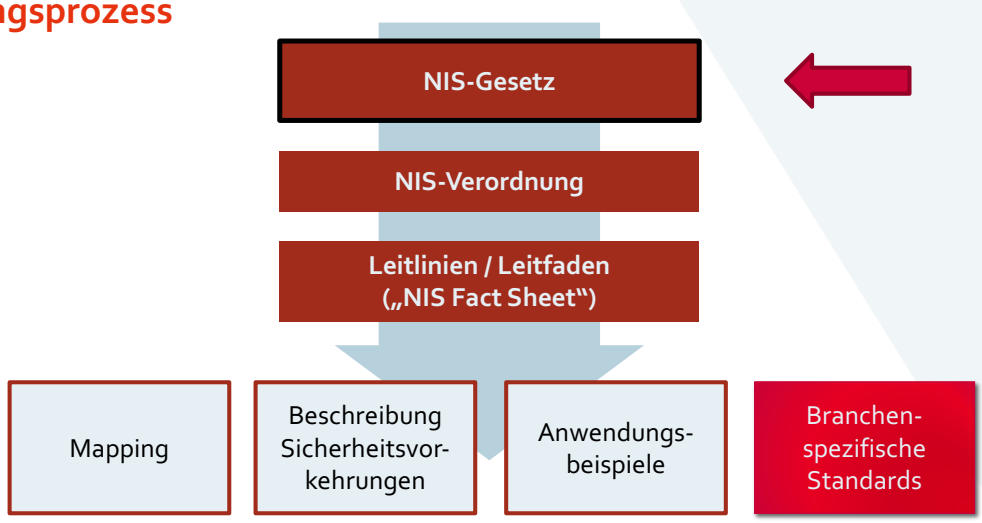
IT-Rechtstag, 23.05.2019

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

Regelungsprozess



IT-Rechtstag, 23.05.2019

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

Definition (NIS-Gesetz)

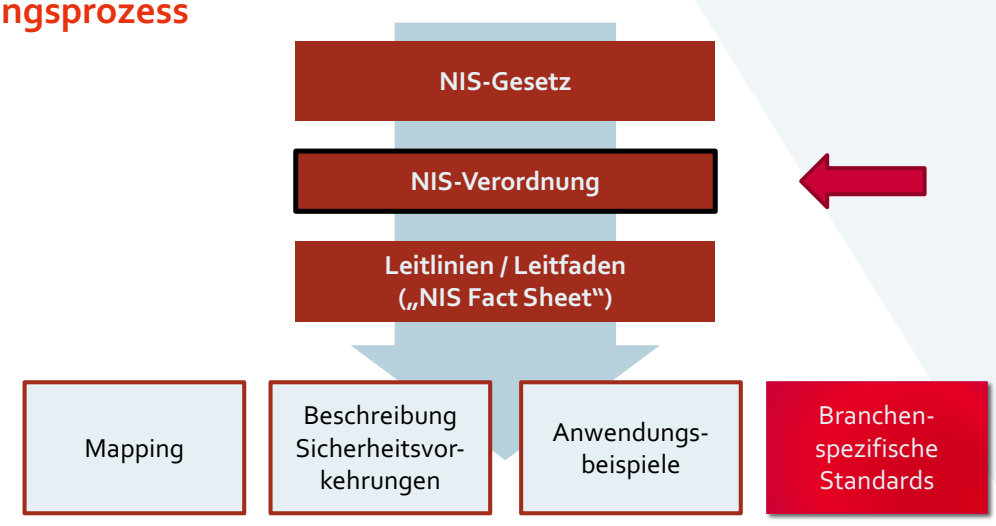
- NIS-Gesetz:
  - Zweck: Gewährleistung der Netz- und Informationssystemsicherheit
  - Gegenstand: Netz- und Informationssysteme
    - die für die Bereitstellung des wesentlichen Dienstes genutzt werden
  - Anforderungen an Sicherheitsvorkehrungen
    - geeignet & verhältnismäßig
    - technischer & organisatorischer Natur
    - berücksichtigen Stand der Technik
    - angemessen zu Risiko, das mit vernünftigem Aufwand feststellbar ist

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

Regelungsprozess

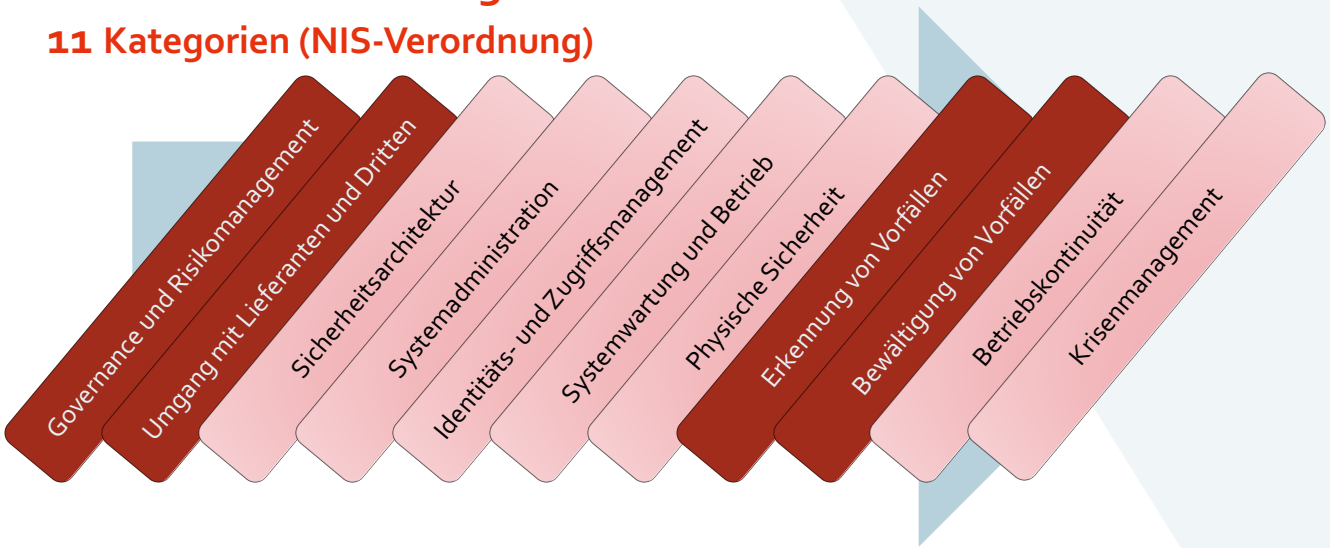


Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

11 Kategorien (NIS-Verordnung)



Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

Sicherheitsmaßnahmen (NIS-Verordnung)

	Sicherheitsmaßnahmen
1.	Governance und Risikomanagement
1.1.	Risikoanalyse: Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.
1.2.	…

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

Regelungsprozess

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

NIS Fact Sheet 08/2018

- **Mapping-Tabelle** von IKT-Sicherheitsstandards und Cyber Security Best Practices (basierend auf Ergebnissen der NIS-Kooperationsgruppe)
  - Österreichisches Informationssicherheitshandbuch Version 4.0.1
  - BSI IT-Grundschutz
  - ISO 27001:2013
  - ISA/IEC 62443 3-3
  - CIS – Critical Security Controls (v6 & v7)
  - NIST Cyber Security Framework

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Sicherheitsvorkehrungen

NIS Fact Sheet 08/2018

- NIS Fact Sheet 08/2018 – Mapping Tabelle, Beispiel:

2.2.1 Governance und Ökosystem

#	Kategorie	Sicherheits-maßnahme	Ö. Informations-sicherheits-handbuch Version 4.0.1	BSI IT-Grundschutz[5]	ISO 27001:2013	ISA/IEC 62443 3-3	CIS CSC Version 6.0	CIS CSC Version 7.0	NIST CYBER SECURITY FRAMEWORK
1	Governance und Risikomanagement	Risikoanalyse	4 Risikoanalyse	*BSI-Standard 100-2, Kapitel 3, 4, 5, BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz*	8.2 Information security risk assessment 8.3 Information security risk treatment	SR 5.1, 5.2, 5.3	1, 2, 4, 13, 14, 17	1, 2, 3, 13, 14, 17	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Überprüfung der Sicherheitsvorkehrungen

Qualifizierte Stellen - Voraussetzungen

„befähigte **Mitarbeiter**"

„adäquate **Zertifizierungen**"

„dem Stand der Technik entsprechende **Werkzeuge**"

„geeigneter **Prüfungsprozess**"

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Überprüfung der Sicherheitsvorkehrungen

Qualifizierte Stellen – befähigte MitarbeiterInnen

- **Fachbereich:** technisch, organisatorisch, techn. & organis.
- QS muss für jede Domain über **mind. 3 Mitarbeiter** verfügen
  - 1 Mitarbeiter mit mehr als 5-jähriger einschlägiger Berufserfahrung
  - 2 Mitarbeiter mit jeweils 3 bis 5-jähriger einschlägiger Berufserfahrung
- **Nachweis von anerkannten Zertifizierungen / Ausbildungen** für den jeweiligen Fachbereich
  - Laufende Weiterbildung der Mitarbeiter
  - Sicherheitsüberprüfung (§§ 55 ff SPG)
    - alle 5 Jahre zu wiederholen

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Überprüfung der Sicherheitsvorkehrungen

Qualifizierte Stellen – adäquate Zertifizierungen

- Zumindest ISO/IEC 27001 oder gleichwertiger Standard

- **Scope:** alle organisatorischen und technischen Prozesse, die im Rahmen der Prüfung von BwD Anwendung finden
- Detailbericht der Zertifizierungsprüfung ist vorzulegen

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Überprüfung der Sicherheitsvorkehrungen

Qualifizierte Stellen – sonstige Erfordernisse

- **Überprüfungen nur durch Prüfer**, die BMI **bekannt gegeben wurden** und deren Eignung im Vorhinein festgestellt wurde;
- Nennung einer **Kontaktstelle** für die Kommunikation mit dem BMI;
- **Unverzügliche Meldung von Vorfällen**, die ihre Netz- und Informationssysteme erheblich stören;
- Einführung eines **Rotationsprinzips** hinsichtlich der Überprüfung;
- **Jährlicher Statusbericht** an BMI über die Tätigkeiten.

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Überprüfung der Sicherheitsvorkehrungen

Qualifizierte Stellen

Prüfberichte qualifizierter Stellen

(„rollierende Teilprüfungen")

Generell: Nachweis der Anforderungen

alle 3 Jahre

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

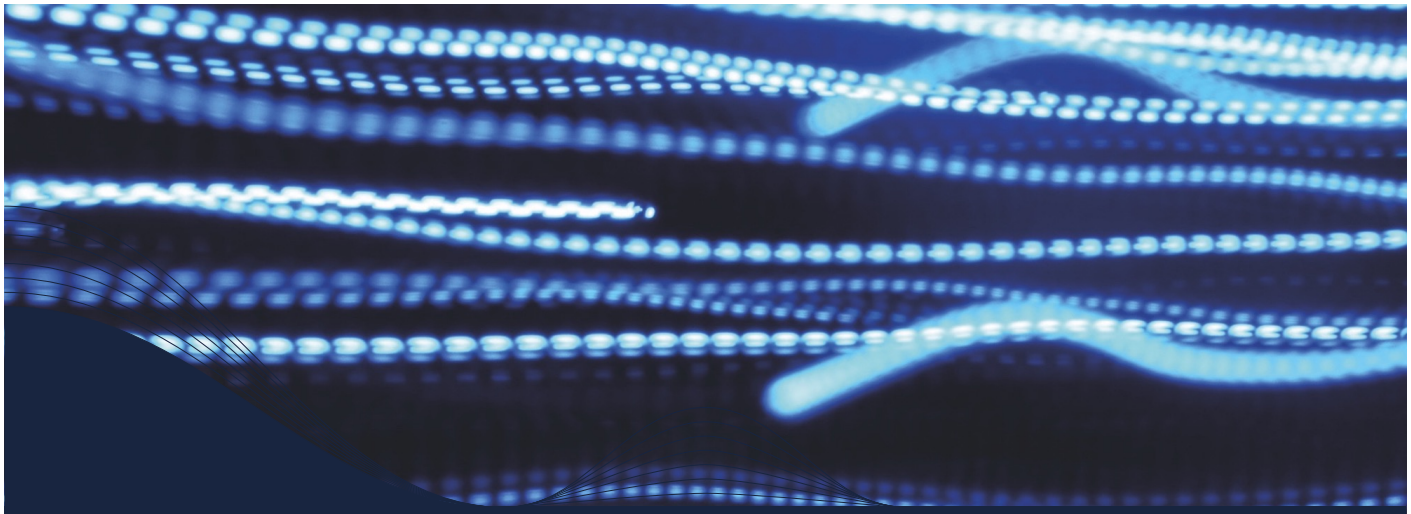
Ausblick

- NIS-Website (https://www.nis.gv.at/)
- Kundmachung und Inkrafttreten der Verordnungen
- Beginn der Ermittlungsverfahren der Betreiber durch BKA
- Eignungsprüfung der Qualifizierten Stellen durch BMI
- Ermittlung sektorenspezifischer Computer-Notfallteams
- Begleitend NIS Fact Sheets
- Begleitend Aktivitäten auf EU-Ebene

Bundeskanzleramt Bundesministerium Inneres

bundeskanzleramt.gv.at
bmi.gv.at

Danke für Ihre Aufmerksamkeit!



Rechtliche Rahmenbedingungen der Cybersecurity

DLA PIPER

Übersicht

i. Unsere Kompetenz
ii. Holistischer Ansatz - "Management Buy-In"
iii. Standards und Entwicklung
iv. Fragen und Diskussion

About DLA Piper

40+
COUNTRIES

90+
OFFICES

$2.63
Global revenue in $USD billions for 2017

225K
Pro bono and community engagement hours donated in 2017

8
GLOBAL PRACTICE AREAS

- Corporate
- Employment
- Finance and Projects
- Intellectual Property and Technology
- Litigation and Regulatory
- Real Estate
- Restructuring
- Tax

10
GLOBAL SECTORS

- Consumer Goods & Retail
- Energy & Natural Resources
- Financial Services
- Industrials
- Infrastructure, Construction & Transport
- Insurance
- Life Sciences
- Media, Sport & Entertainment
- Real Estate
- Technology

Global Presence

AMERICAS
Argentina
Brazil*
Canada
Colombia
Chile
Mexico
Peru
United States

MIDDLE EAST
Bahrain
Kuwait
Oman
Qatar
Saudi Arabia
United Arab Emirates

ASIA PACIFIC
Australia
China
Japan
New Zealand
Singapore
South Korea
Thailand

EUROPE
Austria
Belgium
Czech Republic
Denmark
Finland
France
Germany
Hungary
Italy
Luxembourg
Netherlands
Norway
Poland
Portugal
Romania
Russia
Slovak Republic
Spain
Sweden
Ukraine
United Kingdom

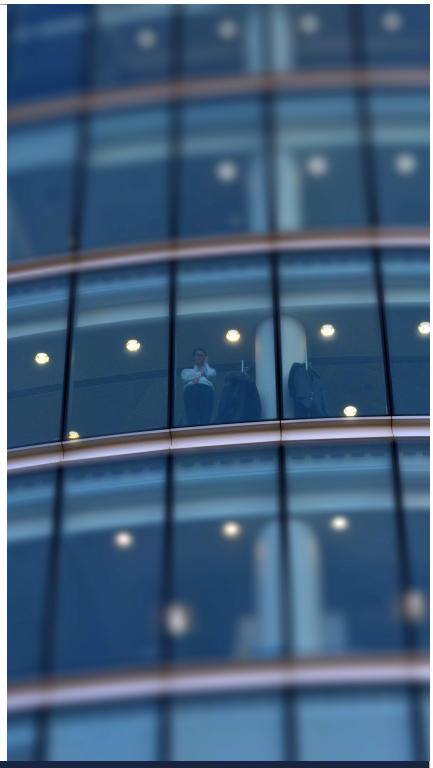
AFRICA
Algeria
Angola
Botswana
Burundi
Ethiopia
Ghana
Kenya
Mauritius
Morocco
Mozambique
Namibia
Nigeria
Rwanda
Senegal
South Africa
Tanzania
Tunisia
Uganda
Zambia
Zimbabwe

Cooperation Firm

Holistischer Ansatz "Management Buy-In"

Cyber-Risiko - die Notwendigkeit einer Aufsicht auf Vorstandsebene

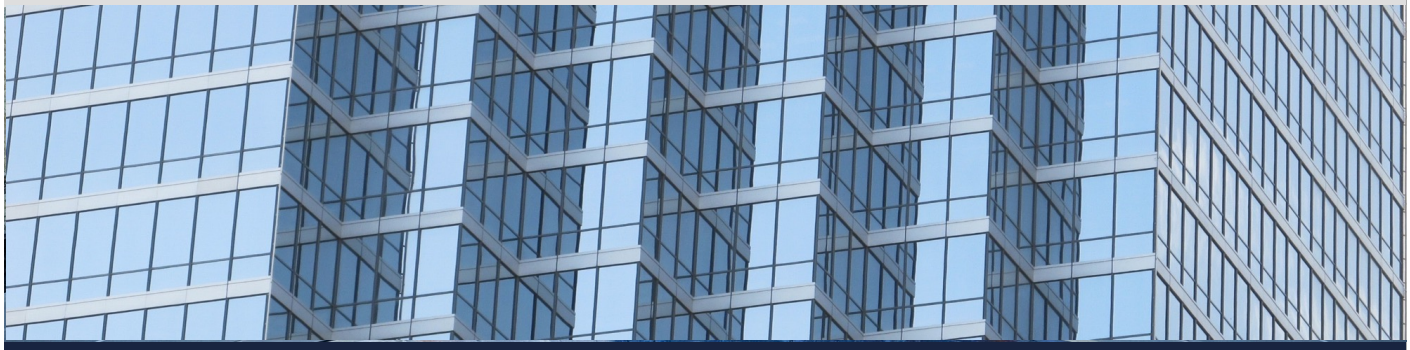
- Komplexes, dynamisches, unternehmensweites Risiko, nicht nur ein IT-Risiko
- Erfordert eine abteilungsübergreifende Wahrnehmung sowie Rollen und Verantwortlichkeiten
- Business Continuity; Risikoeinstellung; die Fähigkeit des Vorstands, das Management zur Rechenschaft zu ziehen
- Vorstand und Unternehmensführung müssen akzeptable Risikobereitschaftsniveaus mit Geschäftszielen wie der digitalen Transformation in Einklang bringen.
- Benötigt ein Cyber-Risikomanagement-Team mit allen maßgeblichen Stakeholder-Abteilungen (einschließlich Recht, Finanzen, HR, IT, F & E und Risikomanagement)
- Behörden beurteilen die Beteiligung des Vorstands



Corporate Liability

Zivilrechtliche Haftung der Gesellschaft

Strafrechtliche Haftung der Gesellschaft



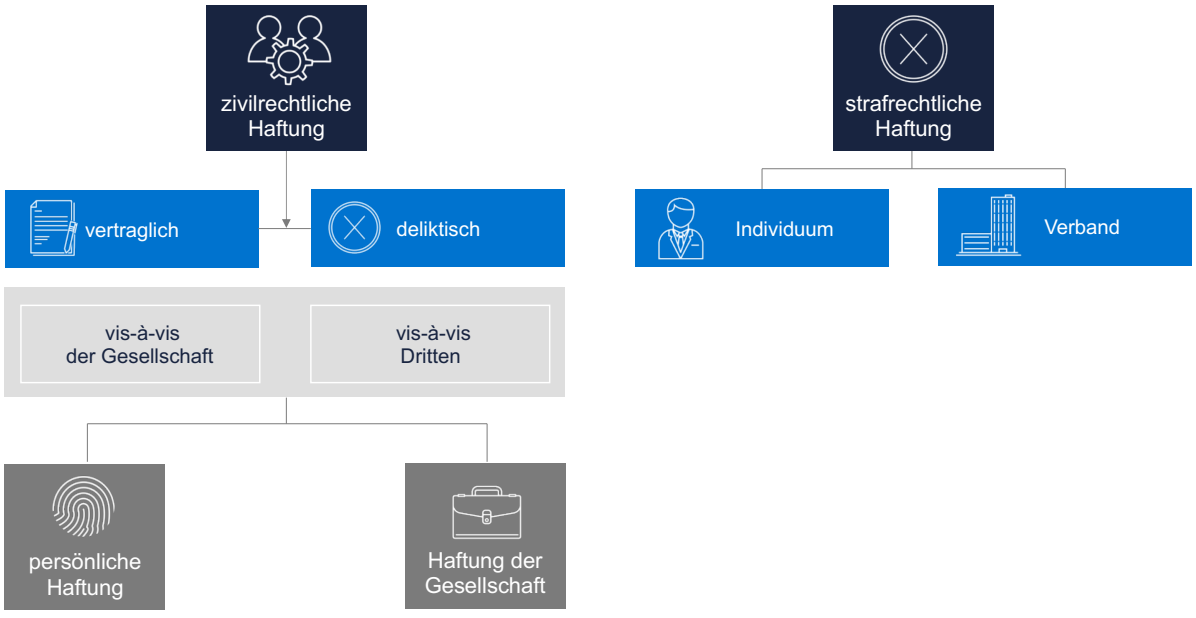
Directors & Officers

Vorstands- und Geschäftsführer-Haftung

Verwaltungs-strafrechtliche Verantwortung

Corporate Governance - Sorgfaltspflichten

Liability Map of a Cyber Incident



Konsequenzen: Intern

Gesellschaft vs. Mitglieder des Vorstands

- Jede Kapitalgesellschaft hat Ansprüche gegen (frühere) Mitglieder des geschäftsführenden Organs geltend zu machen, wenn diese schuldhaft ihre Treuepflichten gegenüber der Gesellschaft verletzt haben.
- Eine D&O Versicherung kann dazu beitragen, die Mitglieder des geschäftsführenden Organs vor einer solchen Haftung zu schützen. Bestehende Richtlinien wurden jedoch möglicherweise nicht mit Blick auf Cyber- und technologiebezogene Risiken abgeschlossen.

Staatsanwaltschaft vs. Verdächtige

Ein strafrechtliches Ermittlungsverfahren kann das Unternehmen für den Beitrag zu einer, durch einen Mitarbeiter, begangenen Straftat ins Visier nehmen wenn die Unternehmensführung die aufgrund der Umstände erforderlichen Treuepflichten missachtet hat, insbesondere indem sie wesentliche technische, organisatorische oder persönliche Maßnahmen zur Verhinderung solcher Handlungen unterlassen hat.

Konsequenzen: Extern

Nach einem Cyber-Incident werden möglicherweise verschiedene Ansprüche geltend gemacht:

Kunden vs. Gesellschaft

- Vertragliche Ansprüche des Kunden wegen schuldhafter Unverfügbarkeit von Leistungen.
- Schadensersatzansprüche wegen Verletzung der DSGVO.
- Sammelklagen und Verbraucherschutzansprüche werden von der Europäischen Union gefördert und in der Regel verfolgt, wenn viele Personen verletzt werden.

Aufsichtsbehörde vs. Gesellschaft und Management

- Die Datenschutzbehörde und andere Behörden können gegen ein Unternehmen und gegen Mitglieder des geschäftsführenden Organs Geldbußen verhängen.
- Behörden können teilweise Abhilfemaßnahmen verhängen, wenn sie die Compliance-Systeme für unbefriedigend halten.

Europarechtliche Meldepflichten

Übersicht Europarechtliche Meldepflichten

	DSGVO	PSD2	NIS
Umfasste Entität	Verantwortliche und Auftragsverarbeiter personenbezogener Daten	Zahlungsdienstleister	Betreiber wesentlicher Dienste und Anbieter digitaler Dienste
Meldepflicht ausgelöst durch	Im Falle einer Verletzung des Schutzes personenbezogener Daten, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.	Im Falle eines schwerwiegenden Betriebs- oder eines Sicherheitsvorfalls wenn sich der Vorfall auf die finanziellen Interessen seiner Zahlungsdienstnutzer auswirkt oder auswirken könnte.	Sicherheitsvorfälle bzw. Störungen mit erhebliche Auswirkungen auf die Verfügbarkeit der bereitgestellten wesentlichen Dienste bzw. auf die Bereitstellung digitaler Dienste.
Berichtszeitraum	innerhalb von 72 Stunden	innerhalb von 4 Stunden	ohne unangemessene Verzögerung
Meldung an betroffene Personen	Ja, eine Meldung ist erforderlich, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.	Ja, wenn der Vorfall Auswirkungen auf die finanziellen Interessen der Verbraucher hat bzw. haben könnte.	Ja, die zuständige Behörde oder das CSIRT können verlangen, dass die Verbraucher informiert werden, wenn eine öffentliche Aufmerksamkeit erforderlich ist oder die Offenlegung im öffentlichen Interesse liegt.

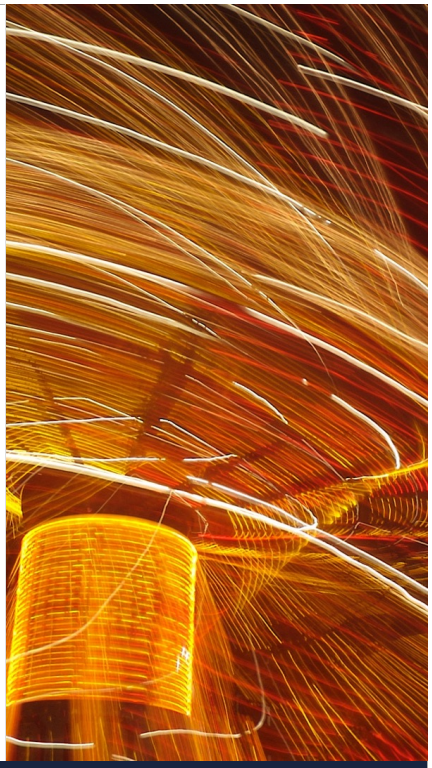
Cyber Incident Compliance: Strafen

Risiko hoher Strafzahlungen

Verletzung der gesetzlichen Offenlegungspflicht:
bis zu EUR 300.000

Verletzung von Aufsichtspflichten:
bis zu EUR 1 Mio.

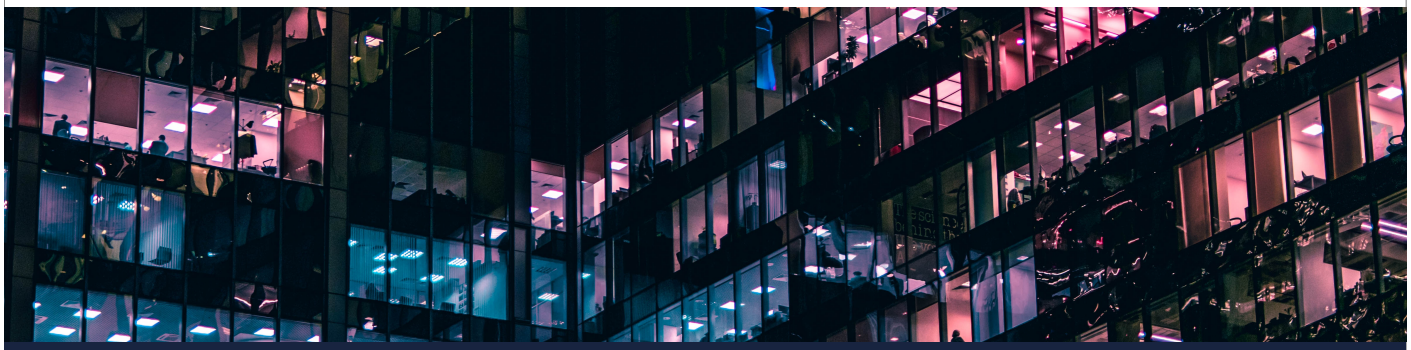
Verstöße gegen die DSGVO bis zu 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes



Das Unternehmen Schützen

Zielsetzung

- Haftung Handelnder minimieren oder ausschließen
- Rechtsnachteile vermeiden
- Rechtsansprüche sichern
- Rechtspflichten in der Krise erfüllen
- Reputationsschäden minimieren



Was heisst "State of the Art" ?

Gesetze vermeiden bewusst die Auflistung bestimmter IT-Standards, um zu verhindern, dass sie veraltet sind

Entwicklung: TIBER-EU Framework (ECB) May 2018

The Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)

Der Rahmenwerk	Zielgebung	Status
Ein gemeinsames Framework, das gestützt auf Informationsanalyse "Red Team-Tests" für kritische Live-Produktionssysteme liefert. "Red-Team-Tests" imitieren die Taktiken, Techniken und Verfahren von realen Bedrohungsakteuren.	• Verbesserung der Widerstandsfähigkeit von Unternehmen und des Finanzsektors gegenüber Cyberangriffen. • Vereinheitlichung und Harmonisierung der Art und Weise, in der Unternehmen in der gesamten EU "Red-Team-Tests" durchführen. • Anleitung für Behörden, wie sie diese Form der Prüfung auf nationaler oder europäischer Ebene einrichten, durchführen und verwalten können.	TIBER ist ein optionaler Rahmen, in dem die zuständige nationale Behörden die aufsichtsrechtlichen Erwartungen der EZB und den aktuellen Fokus auf proaktive Cybersicherheitsmaßnahmen für Finanzinstitute übernehmen können.

Danke für ihre Aufmerksamkeit

Armin Hendrich
Partner
T: +43 (1) 531 78 1561
M: +43 (0) 676 8888 1882
armin.hendrich@dlapiper.com

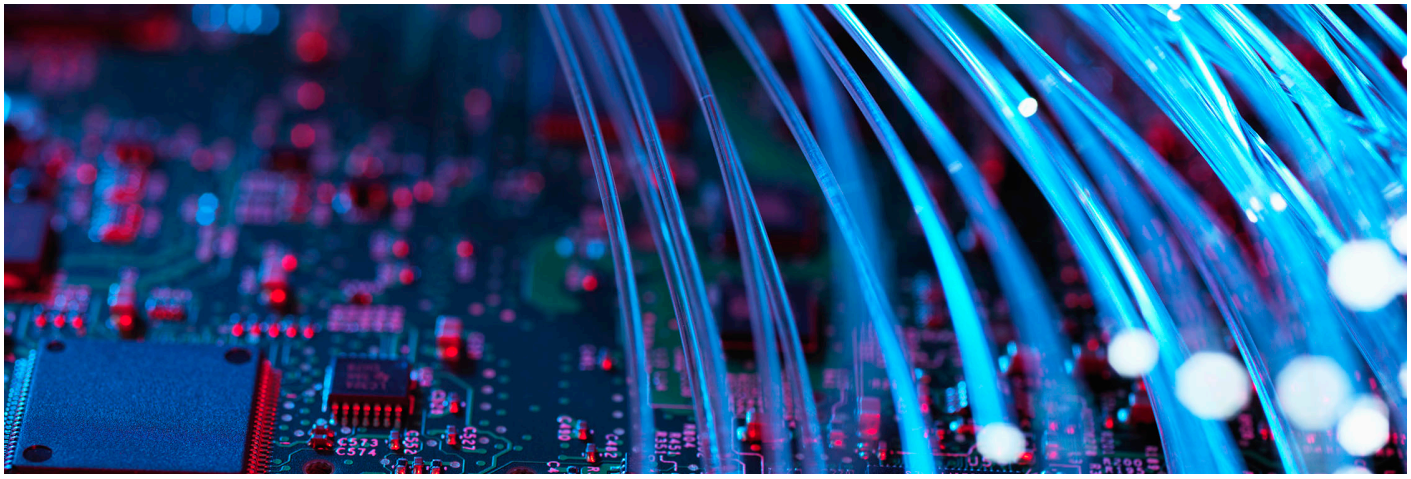
DLA PIPER

Baker McKenzie.

Die E-Evidence VO

13. IT-Rechtstag – 23. Mai 2019

RA Dr. Lukas Feiler, SSCP, CIPP/E



Übersicht

1 E-Evidence-VO: Doping für die Strafverfolgung?

E-Evidence-VO: Doping für die Strafverfolgung?

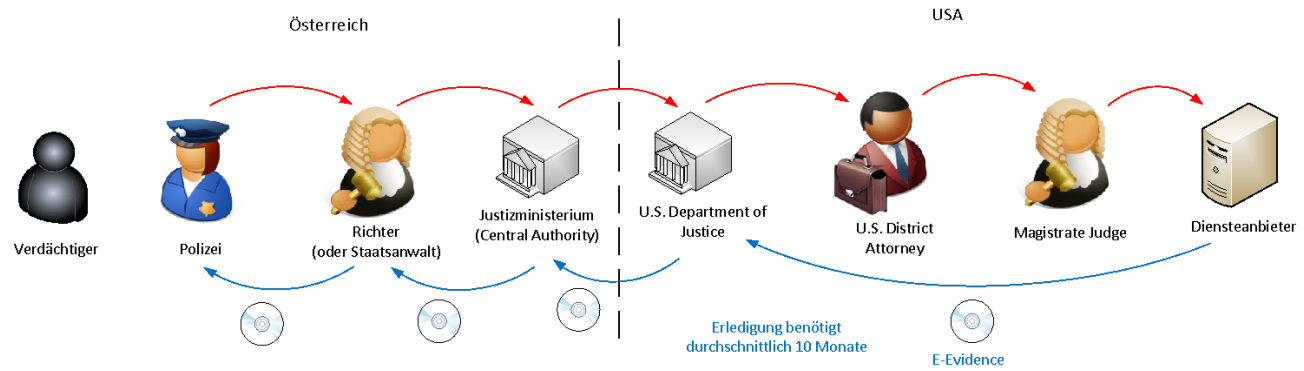
Wahrgenommene Probleme

- **Ineffiziente** Kommunikation zwischen Providern und Behörden
- **Langwierige** Rechtshilfeverfahren
- Täter nutzen (ausländische) Cloud-Dienste und können blitzschnell reagieren

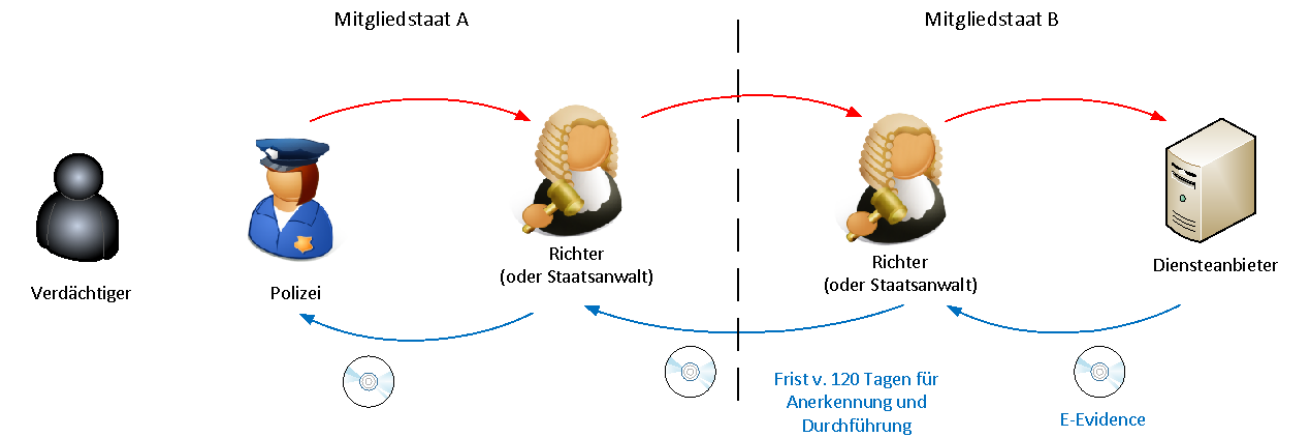
„Lösung“

- E-Evidence-VO – Vorschlang vom 17. April 2018 (Letztfassung vom 12. Dezember 2018)
- Beschleunigtes und vereinfachtes Verfahren – 10 Tage bzw. 6 Stunden
- Geldbußen von bis zu 2% des weltweiten Jahresumsatzes bei Missachtung
- Extraterritorialität

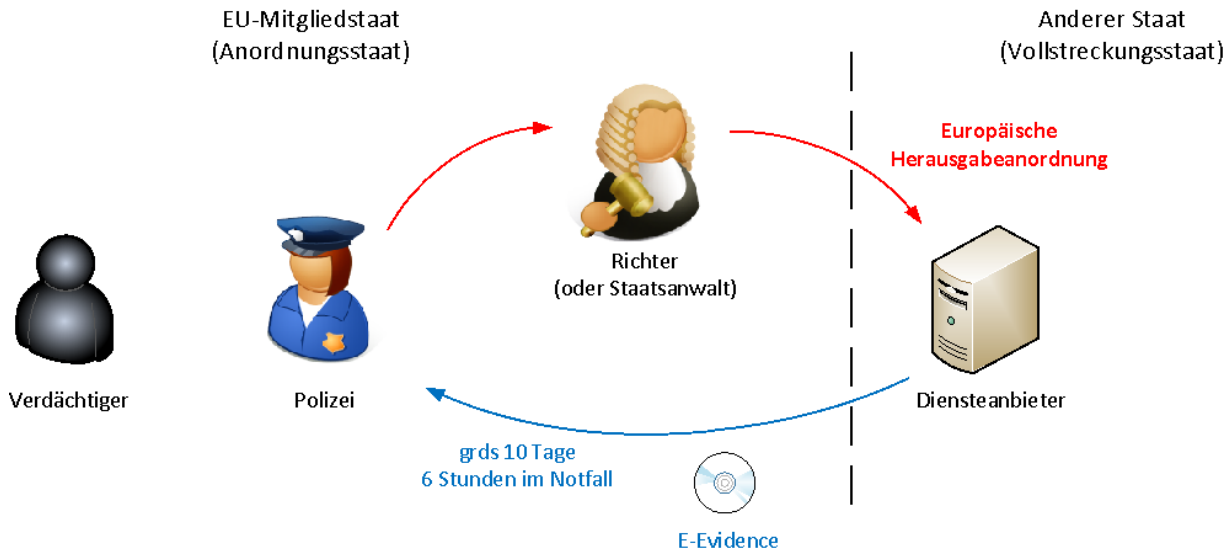
Rechtshilfeabkommen



Europäische Ermittlungsanordnung gem. Richtlinie 2014/41/EU



E-Evidence-VO



2 Anwendungsbereich

Persönlicher & örtlicher Anwendungsbereich

Persönlicher Anwendungsbereich: Diensteanbieter (Art. 3 Abs. 1 iVm Art. 2 Nr.3)

- elektronische Kommunikationsdienste iSd EECC
- Domain Name Registries & Registrars; Proxy Server
- Dienste der Informationsgesellschaft, welche
  - ihren Nutzern die Kommunikation miteinander gestatten oder
  - Daten für die Nutzer verarbeiten oder speichern
- ausgenommen Anbieter von Finanzdienstleistungen

Örtlicher Anwendungsbereich (Art. 3 Abs. 1 iVm Art. 2 Nr. 4)

- sofern in der Union angeboten
  - Nutzung in einem MS ermöglicht
  - Niederlassung in der EU, erhebliche Zahl von Nutzern in EU oder Ausrichtung auf EU
- unabhängig davon, wo sich die Daten befinden (vgl. Art. 1 Abs. 1)

Sachlicher Anwendungsbereich

Beschränkung auf Strafverfahren

- Geltung nur für Strafverfahren und Fahndung nach verurteilten Straftätern (Art. 3 Abs. 2)
  - nur wegen einer konkreten, bereits begangenen Straftat (ErwGr 24); keine Gefahrenerforschung
- Keine Anwendbarkeit bei Rechtshilfeverfahren (Art. 3 Abs. 1a)

Beschränkung auf relevante Daten

- Daten müssen als Beweismittel in Frage kommen und notwendig für die Durchführung des Strafverfahrens sein (ErwGr 29)
- Daten müssen die in der Union angebotene Dienste betreffen (ErwGr 26)

3 Arten der Beweismittel und Anordnungen

Arten der elektronischen Beweismittel

	Teilnehmerdaten (Art. 2 Nr. 7)	Zugangsdaten (Art. 2 Nr. 8)	Transaktionsdaten (Art. 2 Nr. 9)	Inhaltsdaten (Art. 2 Nr. 10)
Definition	Informationen zu • Identität des Kunden oder • Art und Dauer der Dienstleistung	Daten über Beginn und Beendigung der Zugangssitzung eines Nutzers zu einem Dienst (inkl. IP-Adresse, Datum/Uhrzeit der Nutzung)	Kontext- oder Zusatzinformationen zur Erbringung einer Dienstleistung (inkl. wer, wann, mit wem, von welchem Ort aus)	Alle in einem digitalen Format gespeicherten Daten mit Ausnahme von Teilnehmer-, Zugangs- oder Transaktionsdaten
Ungefähre Entsprechung im TKG 2003	Stammdaten (§ 92 Abs. 3 Z 3 TKG)	Zugangsdaten (§ 92 Abs. 3 Z 4a TKG)	Verkehrsdaten & Standortdaten (§ 92 Abs. 3 Z 4 & 6 TKG)	Inhaltsdaten (§ 92 Abs. 3 Z 5 TKG) und sonstige Daten

Europäische Herausgabeanordnung

	Teilnehmerdaten	Zugangsdaten	Transaktionsdaten	Inhaltsdaten
Formelle Voraus-setzungen	• Anordnung (oder Validierung) durch **Richter oder Staatsanwalt** im Anordnungsstaat (Art. 4 Abs. 1) • In Notfällen: Anordnung durch Polizei mit ex post Validierung (Art. 4 Abs. 5)		• Anordnung (oder Validierung) durch **Richter** im Anordnungsstaat (Art. 4 Abs. 2) • In Notfällen: Anordnung durch Polizei mit ex post Validierung (Art. 4 Abs. 5)	
Materielle Voraus-setzungen	• **Jedes Strafverfahren** im Anordnungsstaat • Flüchtiger verurteilter Straftäter, wenn Freiheitsstrafe >= 4 Monate (Art. 5 Abs. 3)		• Strafverfahren wegen Straftat mit **Höchststrafe von >= 3 Jahren** • Bestimmte **harmonisierte Delikte** – gegen Kinder gerichtete Sexualstraftaten – Terrorismusdelikte – Betrug/Fälschung unbarer Zahlungsmittel • Flüchtiger verurteilter Straftäter wegen obiger Delikte, wenn Freiheitsstrafe >= 4 Monate (Art. 5 Abs. 4)	

- Verfügbarkeit einer vergleichbaren nationalen Maßnahme bei Binnensachverhalt (Art. 5 Abs. 2)
- Berücksichtigung von Immunitäten (Art. 5 Abs. 7 und 8)

Europäische Sicherungsanordnung

	Teilnehmerdaten	Zugangsdaten	Transaktionsdaten	Inhaltsdaten
Formelle Voraus-setzungen	• Anordnung (oder Validierung) durch **Richter oder Staatsanwalt** im Anordnungsstaat (Art. 4 Abs. 3)			
Materielle Voraus-setzungen	• Verhältnismäßig, um Löschung oder Änderung zu verhindern und • **Jedes Strafverfahren** im Anordnungsstaat oder • Flüchtiger verurteilter Straftäter, wenn Freiheitsstrafe >= 4 Monate (Art. 6 Abs. 2)			

4 Vollstreckung und Rechtsbehelfe

Zustellung einer Herausgabe-/Sicherungsanordnung

Primär an: Vertreter des Diensteanbieters (Art. 7 Abs. 1)

- Verpflichtung des Diensteanbieters, einen in der EU ansässigen Vertreter zu bestellen (vgl. Begleitrichtline zur E-Evidence VO, COM(2018) 226 final)
- Entgegennahme, Befolgung und Durchsetzung von Anordnungen

Subsidiär an: jene Niederlassung des Diensteanbieters in der Union

- Wenn kein Vertreter benannt wurde (Art. 7 Abs. 2)
- Wenn der Vertreter nicht Folge leistet und (Art. 7 Abs. 3 und 4)
  - ein Notfall vorliegt (Gefährdung von körperlicher Unversehrtheit oder kritischer Infrastruktur) oder
  - ein klares Risiko eines Datenverlustes besteht

Vertraulichkeit und Information von Betroffenen

Pflicht der Diensteanbieter zur Vertraulichkeit (Art. 11 Abs. 1)

- Diensteanbieter darf Verdächtigen nur informieren, wenn Anordnungsbehörde ausdrücklich darum ersucht

Pflicht der Anordnungsbehörde zu Information Betroffener (Art. 11 Abs. 2 bis 4)

- Sobald keine Gefährdung der Ermittlung mehr
- Aufschiebung möglich solange notwendig und verhältnismäßig
- Betroffener ist zugleich über Rechtsbehelfe zu informieren
- Information kann entfallen, wenn dies zum Schutz berechtigter Interessen Dritter erforderlich ist

Vollstreckung – Riskante Ablehnung durch Provider

Diensteanbieter befolgt Anordnung nicht (Herausgabe: binnen 10 Tage, **6h bei Notfall**; Sicherung: unverzüglich)

Spätestens 5 Arbeitstage nach Erhalt: Entscheidung der Vollstreckungsbehörde über Anerkennung (Art. 14 Abs. 2)

Bei Anerkennung: Vollstreckungsbehörde fordert Diensteanbieter zur Befolgung auf und informiert über Ablehnungsmöglichkeit (Art. 14 Abs. 3)

Bei unberechtigter Ablehnung durch Diensteanbieter: Vollstreckung der Anordnung durch Geldbußen bis **2% des weltweiten Umsatzes** (Art. 14 Abs. 6 bis 10)

Binnen 2 Arbeitstagen: Vollstreckungsbehörde leitet erhaltene Daten an die Anordnungsbehörde weiter (Art. 14 Abs. 9)

- offensichtlich nicht von zuständiger Behörde erlassen
- offensichtliche Fehler oder Befolgung faktisch unmöglich
- Diensteanbieter/Daten unterliegen nicht der VO

Beschränkte Rechtsbehelfe gegen Herausgabeanordnungen

Rechtsbehelfe des Diensteanbieters

- Einwand, dass die Anordnung **im Widerspruch zu Rechtsvorschriften eines Drittstaats** steht (Art. 16 Abs. 1) mit aufschiebender Wirkung (Art. 16 Abs. 3)
- Binnen 10 Tage nach Zugang zu erheben (Art. 16 Abs. 2)
- Prüfung zunächst durch die Anordnungsbehörde (Art. 16 Abs. 3)
- Bei Aufrechterhaltung: Prüfung durch das zuständige Gericht des MS der Anordnungsbehörde (Art. 16 Abs. 3 bis 6)

Rechtsbehelfe Betroffener (Art. 17)

- Rechtsbehelfe nach DSGVO und RL 2016/680
- Rechtsbehelfe nach Maßgabe des nationalen Rechts

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 eines Kommentars zur Datenschutz-Grundverordnung und des ersten Praktiker-Buches zur DSGVO sowie des ersten österreichischen DSGVO-Muster-Buches. Er begleitet Unternehmen auf www.digitalwave.at bei der digitalen Transformation.

Handout zum Thema

AI als Erfinder

Fabian Stanke am 13. Österreichischen IT-Rechtstag, 23.-24. Mai 2019

Abgrenzung

Betrachtet wird die patentrechtliche Einordnung von Erfindungen, die von einer Künstlichen Intelligenz (KI, bzw. häufiger englisch Artificial Intelligence, AI) gemacht werden, d.h. im Wesentlichen von einem künstlichen System („inventive AI"). Erfindungen betreffend KI („AI inventions") sind mit völlig anderen Herausforderungen verbunden, die hier nicht Gegenstand sind. Um die Themen nicht zu vermischen, wird davon ausgegangen, dass die hier angenommene erfinderisch aktive KI zum Zeitpunkt der von ihr gemachten Erfindung selbst zum Stand der Technik gehört.

Herausforderungen

Zwei grundlegende Problemfelder ergeben sich aus nicht von Menschen gemachten Erfindungen:

1. Liegt überhaupt eine schutzfähige Erfindung vor oder ist ein maschinell erhaltener Gegenstand per Definition naheliegend?

2. Entsteht an einer solchen Erfindung ein Erfinderrecht und wenn ja, wem?

Schutzfähige Erfindung

Um schutzfähig zu sein, muss eine Erfindung neu sein und „sich für den Fachmann nicht in nahe liegender Weise aus dem Stand der Technik ergeben" (§ 1 Abs 1 PatG). Da wir die KI selbst als bekannt annehmen, könnte der – fiktive – Fachmann sich der KI bedienen, um nach Lösungen zu suchen. Wenn das naheliegend war, und der Fachmann dabei mit vertretbarem Aufwand zu derselben Lösung gelangt wäre, war wohl auch diese Lösung naheliegend. Andernfalls müsste die Erfindung mE als nicht naheliegend anerkannt werden und könnte daher – sofern sie auch die anderen Anforderungen erfüllt, beispielsweise Technizität – schutzfähig sein.

Erfinderrecht

„Auf die Erteilung des Patentes hat nur der Erfinder oder sein Rechtsnachfolger Anspruch" (§ 4 Abs 1 PatG). Nach hM können Erfinder nur natürliche Personen sein, wobei damit juristische Personen ausgeschlossen werden sollten, und nicht etwaige „elektronische Personen". Das Recht an der Erfindung entsteht durch den Erwerb des Erfindungsbesitzes. Es kommen daher folgende mögliche Erfinder in Betracht:

1. Die KI als „electronic person";

2. Die Schöpfer der KI, d.h. die Entwickler oder Programmierer der KI;

3. Die Eigentümer der KI, d.h. die Besitzer oder Betreiber der KI;

4. Die Trainer der KI, d.h. jene Personen, die die KI mit Eingaben und Daten versorgen; oder

5. Die Benutzer der KI, d.h. jene Personen, die die KI zur Lösung eines Problems einsetzen.

Schlussfolgerung

ME spricht derzeit vieles für die Benutzer der KI:

- Die Benutzer erkennen in der Regel als erste die Erfindung als solche und sind die ersten natürlichen Personen im Erfindungsbesitz. Eine Erweiterung auf elektronische Personen wäre mE nicht zweckmäßig, weil diese für den volkswirtschaftlich gewünschten Anreiz zur Offenlegung von Erfindungen im Tausch für ein temporäres Monopol im Allgemeinen nicht empfänglich sind.

- Da die Benutzer auf die Eigentümer und indirekt auch auf die Trainer und Schöpfer angewiesen sind, können diese ihren Anteil an etwaigen Erfindungsrechten der Benutzer jeweils vertraglich sichern.

- Sofern die vom Benutzer definierte Aufgabenstellung nicht naheliegend ist (so genannte Aufgabenerfindung) sollten die Erfinderrechte jedenfalls hier liegen.

- Gegen ein Erfinderrecht bei den Schöpfern der KI spricht, dass diese ohnehin Aspekte der KI schützen können und auch außerhalb von KI Erfinder eines z.B. mechanischen Werkzeugs nicht Erfinder aller damit geschaffener Gegenstände sind.

- Gegen ein Erfinderrecht bei den Trainern spricht, dass auch Eltern oder Lehrern von (natürlichen) Erfindern keine Erfinderrechte entstehen.

Bei dieser Variante würden allerdings bei Erfindungen keine Erfinderrechte entstehen, die spontan von einer KI gemacht werden, d.h. ohne eine Aufgabenstellung von einem Benutzer.

Gelegentlich wird argumentiert, dass das Erfinderrecht den Eigentümern zustehen soll. Dafür spricht, dass diese einen berechtigten Wunsch nach Investitionssicherheit hinsichtlich ihrer Investitionen in die KI haben. Sofern spontane Erfindungen (ohne Benutzer) betroffen sind, für die sonst keine Erfinderrechte entstünden, wäre diese Variante mE zweckmäßig und in Anlehnung an den Übergang von Erfinderrechten von Dienstnehmern auf ihre Dienstgeber zu regeln.

schönherr
ATTORNEYS AT LAW

Initial Coin Offerings
Technische Einführung und rechtliche Probleme

13. Österreichischer IT-Rechtstag 2019

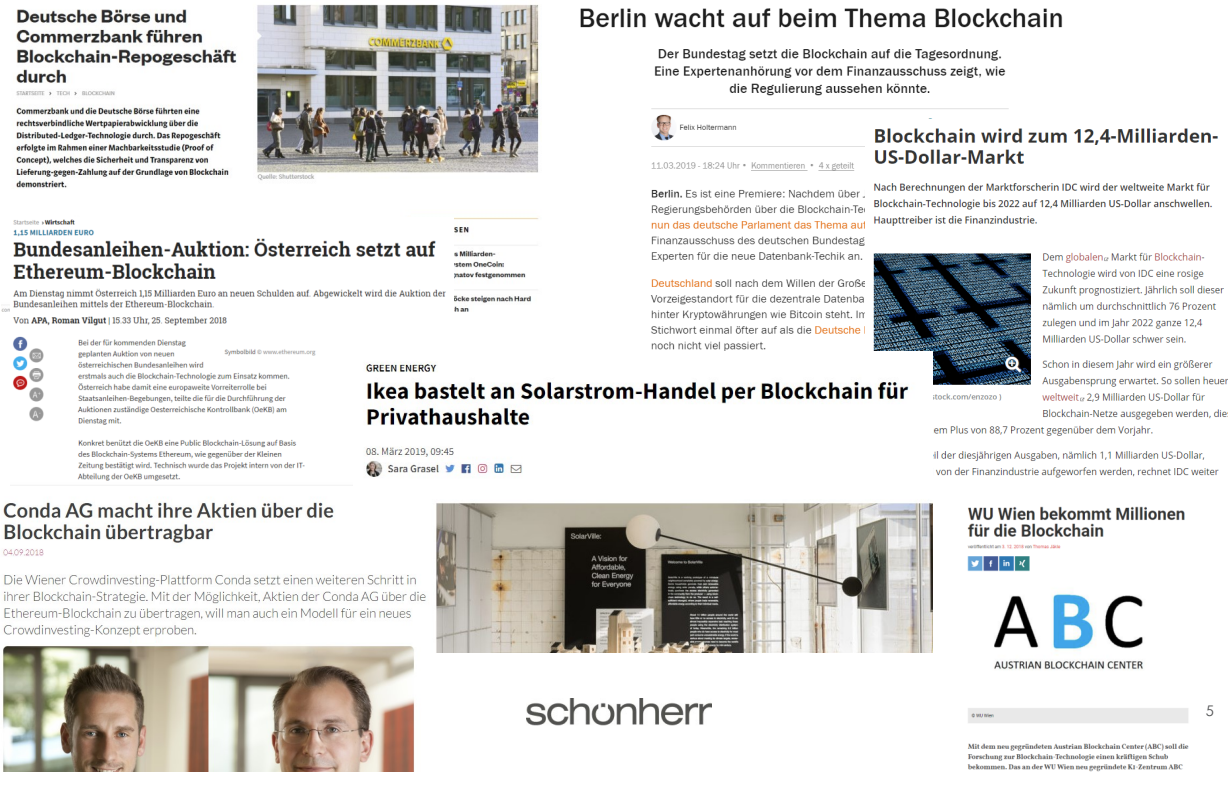
Dr. Thomas Kulnigg
23.05.2019

Agenda

- Teil 1: Einführung in die Blockchain Technologie (Blockchain 101) (15 min)
- Teil 2: Finanzierung über die Blockchain aus rechtlicher Sicht (30 min)

Teil 1: Einführung in die Blockchain Technologie

Blockchain Everywhere



Blockchain 101

- *Distributed Ledger Technology* (***DLT***) = Verteile Datenbank in einem elektronischen Peer-to-Peer Netzwerk
  - Blockchain ist bekannteste DLT-Anwendung
  - Bitcoin und Ehtereum sind bekannteste Blockchains
- Jeder Netzwerk-Knoten (*Node*) unterhält eine **gleichgestellte Kopie** der Datenbank
- Neue Einträge in der Datenbank werden in alle Kopien der Datenbank übernommen, wenn entsprechende **Übereinkunft (Konsensus)** im Netzwerk besteht
  - Keine zentrale (clearing) Stelle
  - **Vermeidung von Double Spending**

Konsensus Mechanismen

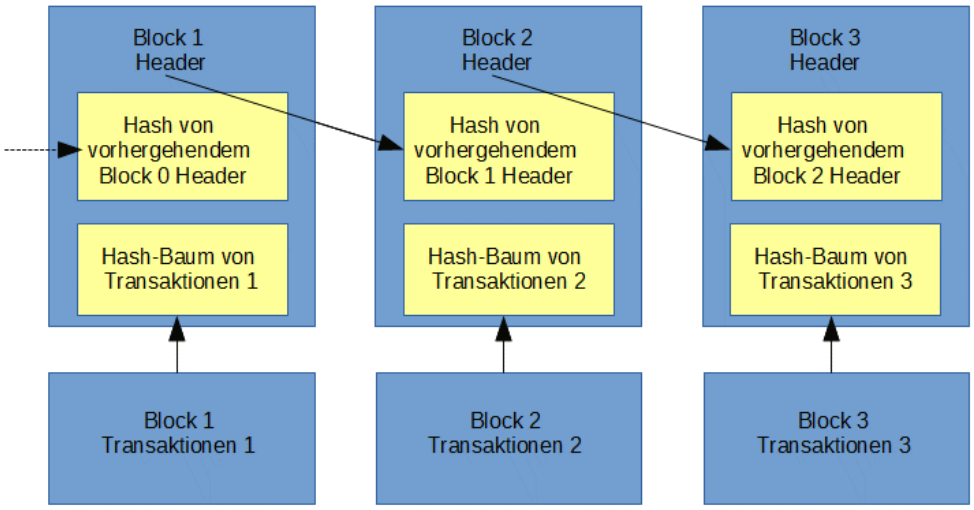
- Notwendig, um verteiltes Netzwerk zu organisieren („corporate governance"-Regeln/Bylaws)
- Unterschiedliche Mechanismen existieren in Theorie und Praxis
- Proof of Work
  - Lösung einer schweren Aufgabe (= vertrauensbildende Maßnahme), leichte Überprüfbarkeit („Mining"; zB Bitcoin, Ethereum)
  - Nachteile: hoher Stromverbrauch, hoher Hardware-Aufwand → Belohnungssystem notwendig (Token Economy); Manipulation durch dominante Teilnehmer (Mining-Farmen)
- Proof of Stake
  - Generelle Gleichberechtigung der Teilnehmer; Entscheidung, welcher Teilnehmer den nächsten Block erzeugen darf zB durch gewichtete Zufallsauswahl

Besonderheiten einer Blockchain

- Block-Struktur = gebündelte Datensätze, die miteinander verkettet sind
- Sicherheit: Fälschungssicherheit durch kryptographische Verfahren bei der Validierung
- Konsensus Mechanismus / Validierung – typischerweise via „Proof of Work"
  - Bitcoin: Mining Nodes (lösen kryptographisches Rätsel), Validation Nodes (überprüfen Richtigkeit der Hashfunktionen)
- Token Economy (Incentivierung durch Ausgabe von Token)
- Transparenz, Offenheit
  - Private vs. public / Permissioned vs. Permissionless
- Wallet: public vs. private key

Besonderheiten einer Blockchain

Vereinfachte Bitcoin-Blockchain



Quelle: https://commons.wikimedia.org/wiki/File:Bitcoin_Developer_Guide_Vereinfachte_Bitcoin_BlockChain_D.gif

Smart Contracts

- = dezentrale Anwendungen/Computerprotokolle; technische Abwicklung z*B* eines (wenn → dann) (Rechts-)Verhältnisses
- Automatische Überprüfung des Eintritts der vertraglichen Konditionen
  - Technologie soll für Einhaltung des Vertrags sorgen
- Abwicklung via Blockchain, d.h. volle Transparenz und Manipulationssicherheit
- Beispiel Ethereum:
  - Plattform für Kryptowährung Ether und für Smart Contracts
  - Smart Contracts agieren autonom wie Accounts (self-executing); keine nachträgliche Änderung möglich (problematisch bei Fehlern im Code)
  - Erstellung von Token durch Smart Contracts (dApp tokens / DAO tokens)
- Transaktionsgebühren (Gas)

Token

- Token = Datensatz (Datenpaket), digitale Einheiten
  - Native Tokens: Bitcoin, Ether (Coins)
  - Ethereum: App Tokens aka „Token“ = Smart Contract
- Übertragbarkeit, Handelbarkeit
- Kein herkömmliches Mining
  - Beliebige Erstellung
- Unterschiedlichste Ausgestaltungen
- Können (technisch) Vermögenswerte repräsentieren
- Zivilrechtlich: unkörperliche Sache (?)

Mögliche Blockchain Anwendungen

- Finanzwelt: Währungen, Finanzierung (ICOs, STOs), Zahlungsabwicklung, Abwicklung von Transaktionen
- Verwaltung von IP-Rechten, Schutz von Ideen (Timestamp)
- Verwaltung von (sensiblen) Daten
- Wahlen, Ausübung von Bürgerrechten
- „Miteigentum“ an „Off-Chain Vermögensgegenständen“ (Gemälde, Grundstücken, Diamanten, etc)
- Autonomes Fahren
- Etc… → jede Datenbankanwendung!

Teil 2: Finanzierung über die Blockchain

schönherr

Finanzierung über Blockchain

- ICO = Initial Coin Offering (alt.: „Token Generating Event“)
  - Emittent begibt Blockchain (DLT) Token
  - Investor bezahlt mit Krypto-Asset (zB Bitcoin, Ether)
  - Unternehmens- oder Projektfinanzierung
  - Meist Eigenemission, Abwicklung via Blockchain
  - Oft nicht reguliert
- Boom 2016-2018
- Seit 2018: vermehrt Security Token Offerings
  - Regulierung anwendbar
- 2019: Initial Exchange Offerings
  - Abwicklung des ICOs über Exchange Plattform

Finanzierung über Blockchain

- ICO vs. STO vs. IPO
  - ICO vs. STO
    - Utility Token („Gutschein“) vs. Security Token (Wertpapier)
    - Ablauf und Abwicklung sind gleich/ähnlich
  - STO vs. IPO
    - In beiden Fällen: Wertpapiere
    - STO: Abwicklung via Blockchain (Smart Contract); IPO: Abwicklung idR via Investmentbank/Intermediär
    - bei STO: kein Börselisting (noch)

Ablauf ICO/STO

- Vorbereitungen
  - Rechtliche Analyse, Erstellung Whitepaper, Ts&Cs, Kauf-/Tauschverträge, Definition Token, SmartContract, Marketingkampagne, etc.
- Pre-ICO/STO
  - Private Sale/Pre-Sale (Bonus/Discount)
  - STO: Genehmigung Kapitalmarktprospekt (falls notwendig)
- Crowdsale (ICO/STO)
- Token Distribution/Activation
- Post-ICO/STO

Rechtliches

- Aufsichtsrechtliches „Minenfeld“
  - FMA: technologie-neutraler Ansatz
- Token werden in Kategorien unterteilt, um regulatorische Einordnung zu erleichtern:
  - Security Token
  - Utility Token und
  - Payment Token
- Oft keine eindeutige Einordnung möglich → Einzelfallbetrachtung

schönherr

Rechtliches

- Security Token
  - Ansprüche auf Auszahlungen gegenüber dem Emittenten (Geld oder Kryptowährung)
  - Gesellschafsrechtliche oder schuldrechtliche Basis
  - Die Ausgestaltung solcher Security Token ähnelt somit jener von „klassischen Wertpapieren“, insbesondere Anleihen oder Aktien. Security Token werden somit häufig als Wertpapiere im Sinn des KMG sowie des WAG 2018 anzusehen sein.
  - Auch Veranlagung ist möglich.
- Relevante regulatorische Vorschriften: KMG/AltFG, WAG 2018, DepotG, BWG, AIFMG, etc.

schönherr

Rechtliches

- Exkurs: Schwellenwerte für öffentliche Angebote

Schwellenwerte (12 Monate Betrachtungszeitraum)	Wertpapiere	Veranlagungen
Unter 250.000 €	Keine Prospektpflicht, keine Informationspflicht nach AltFG	
Ab 250.000 € bis 2 Mio €	Anwendbarkeit AltFG Grenze: emittierter Gesamtgegenwert in der Europäischen Union erreicht oder übersteigt 5 Mio € binnen zwölf Monaten (dann Prospektpflicht nach KMG)	Anwendbarkeit AltFG Grenzen: aushaftender Betrag überschreitet 5 Mio € binnen sieben Jahren (dann Prospektpflicht nach KMG) oder emittierter Gesamtgegenwert in der Europäischen Union erreicht oder übersteigt 5 Mio € binnen zwölf Monaten (dann Prospektpflicht nach KMG)
Ab 2 Mio € bis 5 Mio €	KMG-Prospekt unter der Prospektbilligung durch die FMA (§ 8a KMG; Inland); optional EU-Prospekt (zwecks Passporting)	Vereinfachter KMG-Prospekt nach Schema F oder Prospekt gemäß § 8 KMG nach Schema C
Ab 5 Mio €	EU-Prospekt mit FMA-Billigung	KMG-Prospekt ohne FMA-Billigung nach Schema C

Rechtliches

- Payment Token
  - Primärer Zweck: Bezahlfunktion
- Relevante regulatorische Vorschriften: BWG, E-Geld Gesetz, ZaDiG.
  - Ausnahmen: begrenzte Netze (kleine, spezifische Netze sollen nicht unter strenge Aufsichtsgesetze fallen)

Rechtliches

- Utility Token
  - Nutzen in Hinblick auf ein bestimmtes Produkt oder eine Dienstleistung
  - „Gutschein“
  - Achtung: Hybride Ausgestaltung / schwierige Einordnung
- Bei „sauberer“ Ausgestaltung: kein aufsichtsrechtlicher Anknüpfungspunkt

Rechtliches

- Anleger/Konsumentenschutz
- Zivilrechtliche Fragestellungen (Vertragsabschluss, sachenrechtliche Einordnung von Token, Haftung)
- Handelbarkeit/“Listing“?
- AML/KYC Vorschriften
- FAGG/Rücktrittsrecht
- Informationspflichten

schönherr
ATTORNEYS AT LAW

Schoenherr is one of the top corporate law firms in Central and Eastern Europe. With our wide-ranging network of offices throughout CEE/SEE, we offer our clients unique coverage in the region. The firm has a long tradition of advising clients in all fields of commercial law, providing seamless service that transcends national and company borders. Our teams are tailor-made, assembled from our various practice groups and across our network of offices. Such sharing of resources, local knowledge and international expertise allows us to offer the client the best possible service. www.schoenherr.eu

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Zahlen mit Daten

–

Vertragsrechtliche Fragen

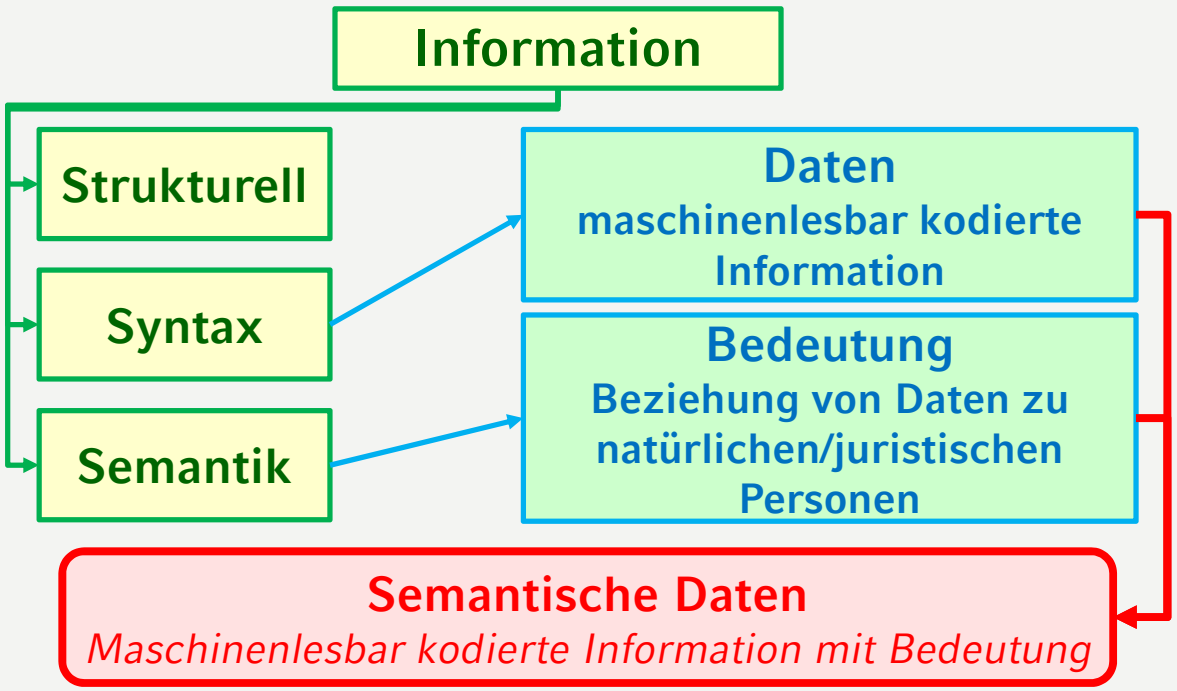
13. Österreichischer IT-Rechtstag, Wien
23. Mai 2019

Dr. Andreas Sattler, München

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

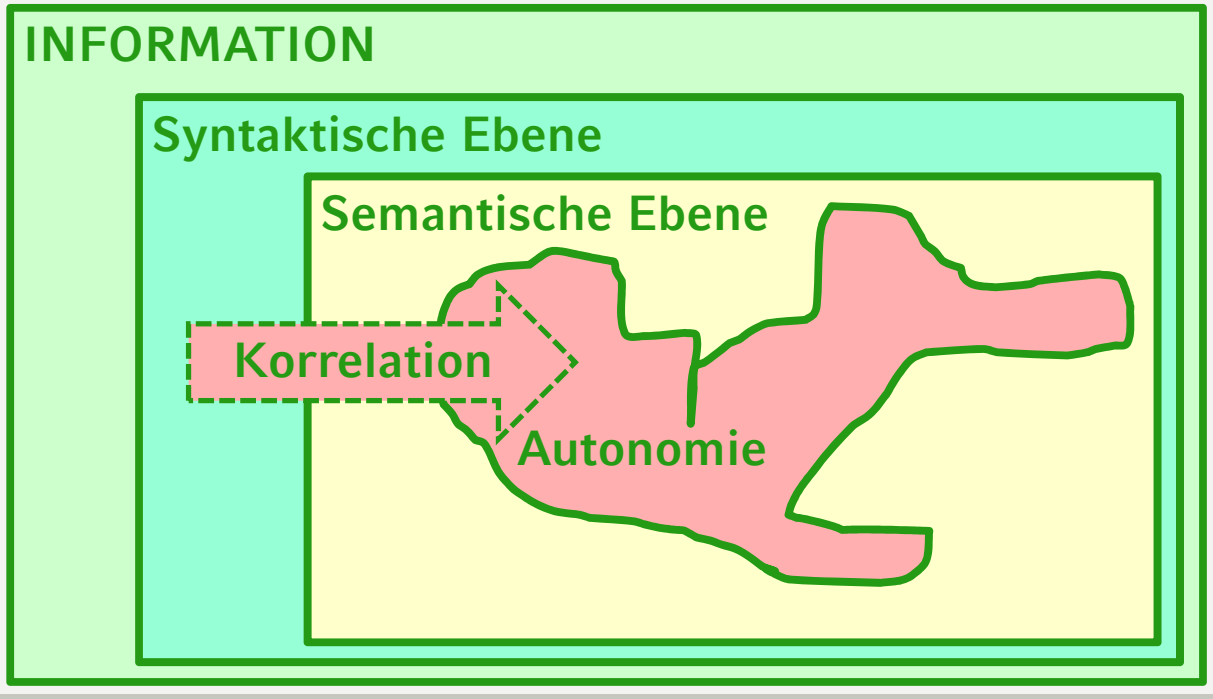
Gliederung

Begriff „Daten“



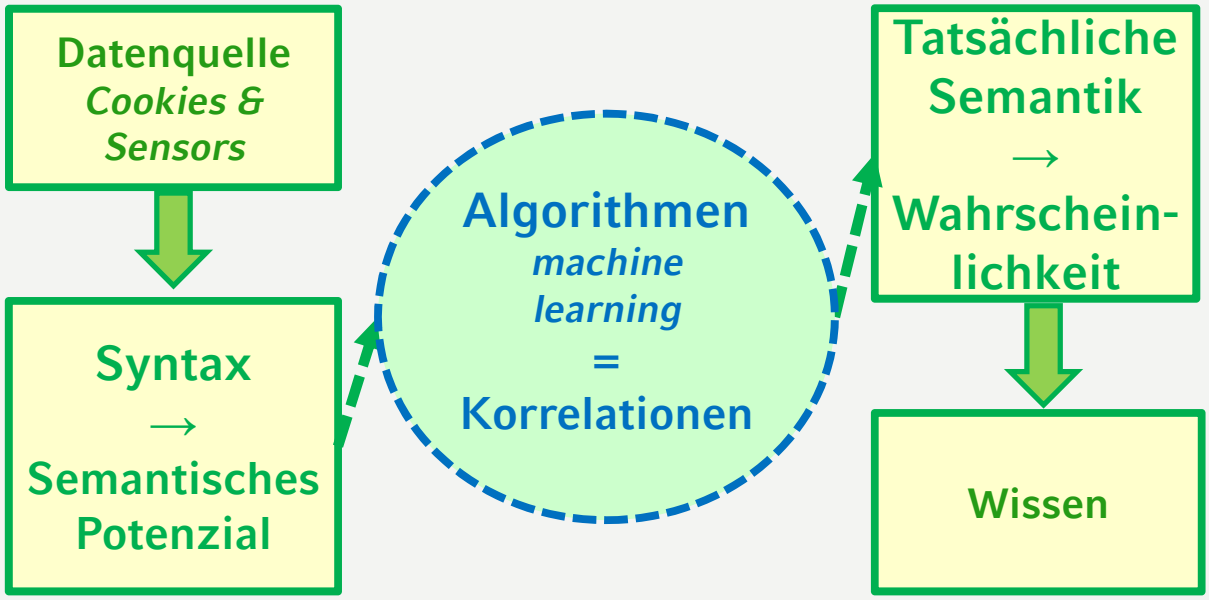
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Begriff „Daten“



Dr. Andreas Sattler

Begriff „Daten“



Gliederung

Art. 4 Nr. 1 DSGVO

Information, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, mittels eines Merkmals identifiziert werden kann.

Dynamische IP-Adresse = Personenbezug,

wenn der Website-Betreiber sie speichert und er über rechtliche Mittel verfügt, die vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.

EuGH – *Breyer/Deutschland* (Rn. 48)

Art. 6 I Uabs.1 DSGVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist […]“

Art. 9 DSGVO

„(1) Die Verarbeitung [sensibler] personenbezogener Daten, […] ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen: […]“

sog. Verbot mit Erlaubnisvorbehalt

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gliederung

I. **Begriff der Daten**

   1. *Personenbezogene Daten*

   2. ***Maschinengenerierte Daten***

II. Gestaltungen von Datenverträgen

III. Fazit

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Maschinengenerierte Daten
(ohne Personenbezug)

§ 76c UrhG

„Eine **Datenbank** (§ 40f Abs. 1) genießt den Schutz nach diesem Abschnitt, wenn für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts eine nach Art oder Umfang wesentliche Investition erforderlich war."

§ 26b UWG

Geschäftsgeheimnis ist eine Information, die
1. geheim ist,
2. von kommerziellem Wert ist, weil sie geheim ist, und die
3. Gegenstand von angemessenen Geheimhaltungsmaßnahmen ist.

Erlaubnis mit Verbotsvorbehalt

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gliederung

I. Begriff der Daten

II. Vertragsrechtliche Gestaltungsfragen

III. Fazit

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

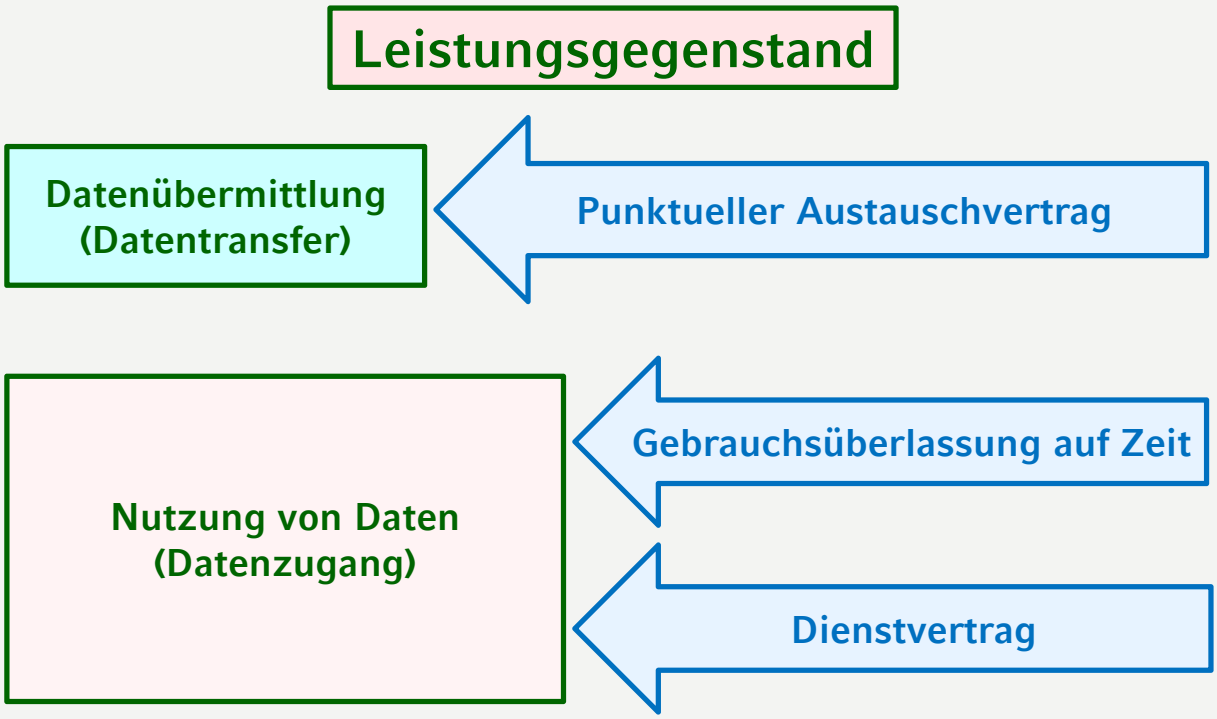
Gestaltungsfragen 1

„Zahlen mit Daten“

1. Keine Verfügungen über absolute Rechte:
→ Kein „Recht am eigenen Datum“
→ Kein „Recht des Datenerzeugers“

2. Keine „Krypto-Währungen“

3. Daten als Leistungsgegenstand
→ Ausschließlich Daten als (Gegen-)Leistung
→ Gemischte (Gegen)Leistung (Geld und Daten)
→ Daten gegen Daten:
- digitale Inhalte gegen personenbezogene Daten
- Maschinendaten gegen Maschinendaten



Gliederung

I. Begriff der Daten

II. Vertragsrechtliche Gestaltungsfragen

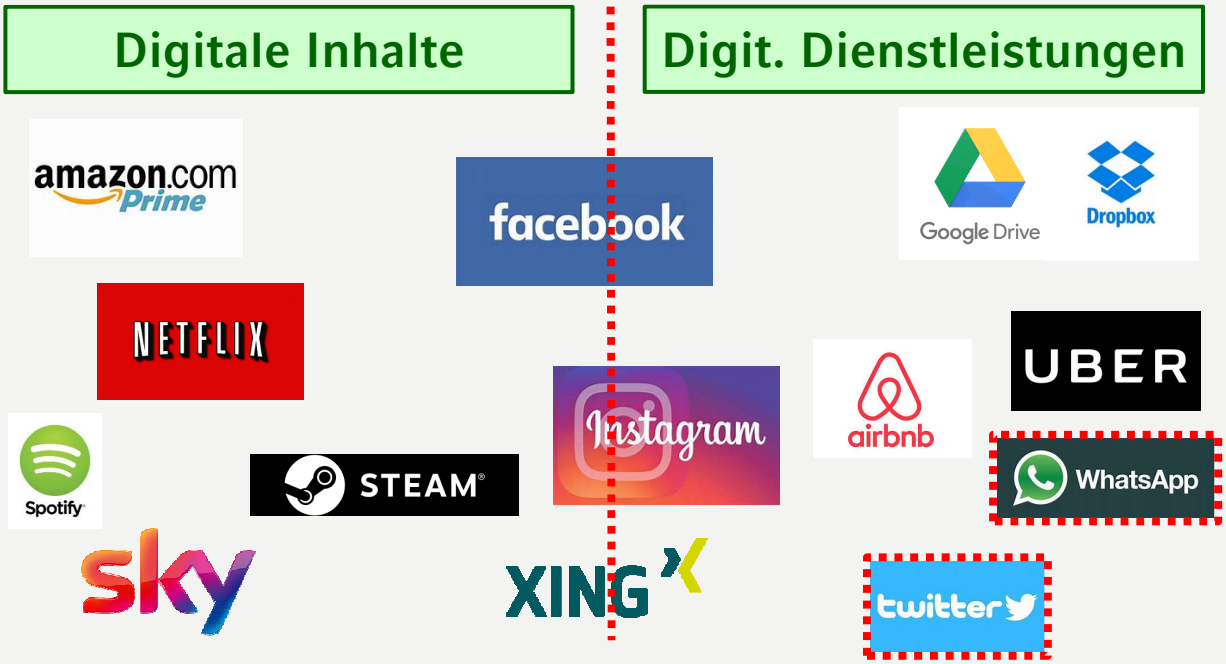
1. Personenbezogene Daten

2. Maschinengenerierte Daten

III. Fazit

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gestaltungsfragen
→ *personenbezogene Daten 1*

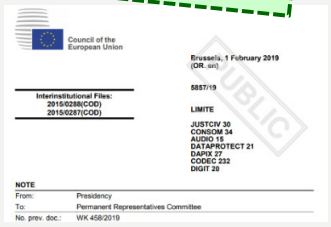


LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gestaltungsfragen
→ *personenbezogene Daten 2*

Unionsrecht

Digital Inhalte und digitale Dienstleistungen RL (2019)



Council of the European Union

Brussels, 1 February 2019 (OR. en)

5857/19

Interinstitutional Files: 2015/0288(COD) 2015/0287(COD)

LIMITE

JUSTCIV 30
CONSOM 34
AUDIO 15
DATAPROTECT 21
DAPIX 27
CODEC 232
DIGIT 20

PUBLIC

NOTE

From: Presidency
To: Permanent Representatives Committee
No. prev. doc.: WK 458/2019

Artikel 3

Anwendungsbereich

(1) Diese Richtlinie gilt für alle Verträge, auf deren Grundlage der Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienstleistungen bereitstellt oder deren Bereitstellung zusagt und der Verbraucher einen Preis zahlt oder dessen Zahlung zusagt.

Diese Richtlinie gilt auch, wenn der Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienstleistungen bereitstellt oder deren Bereitstellung zusagt und der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt, außer in Fällen, in denen die vom Verbraucher bereitgestellten personenbezogenen Daten durch den Unternehmer ausschließlich zur Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen im Einklang mit dieser Richtlinie oder zur Erfüllung von vom Unternehmer einzuhaltenden rechtlichen Anforderungen verarbeitet werden und der Unternehmer diese Daten zu keinen anderen Zwecken verarbeitet.

(8) Das Unionsrecht betreffend den Schutz personenbezogener Daten gilt für alle personenbezogenen Daten, die im Zusammenhang mit Verträgen gemäß Absatz 1 verarbeitet werden.

Insbesondere lässt diese Richtlinie die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt. Im Fall von Widersprüchen zwischen Bestimmungen dieser Richtlinie und dem Unionsrecht zum Schutz personenbezogener Daten ist letzteres maßgeblich.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gestaltungsfragen
→ *personenbezogene Daten 3*

Digitale Inhalte RL Vorschlag der EU-Kommission 2015


EUROPEAN COMMISSION

Brussels, 9.12.2015
COM(2015) 634 final
2015/0287 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on certain aspects concerning contracts for the supply of digital content

ErwG

13/14/37/42: „Gegenleistung"

Anwendungsbereich

Art. 3 I: Auch anwendbar, wenn der Verbraucher die Gegenleistung nicht in Geld, sondern in Form von (personenbezogene) Daten leistet.

Vertragsbeendigung

Art. 13 II lit.b: Weiternutzung, soweit für Vertragsdurchführung mit anderen Kunden erforderlich.

Digitale Inhalte und Dienstleistungs RL (2019)


Council of the European Union

Brussels, 1 February 2019

8887/19

LIMITE

JUSTCIV 39
CONSOM 94
COMER 34
DATAPROTECT 21
DAPIX 27
CODEC 232
DIGIT 20

PUBLIC

NOTE
From: Presidency
To: Permanent Representatives Committee
No. prev. doc.: WK 450/2019

ErwG

24: Keine Ware ("no-commodity")

Anwendungsbereich

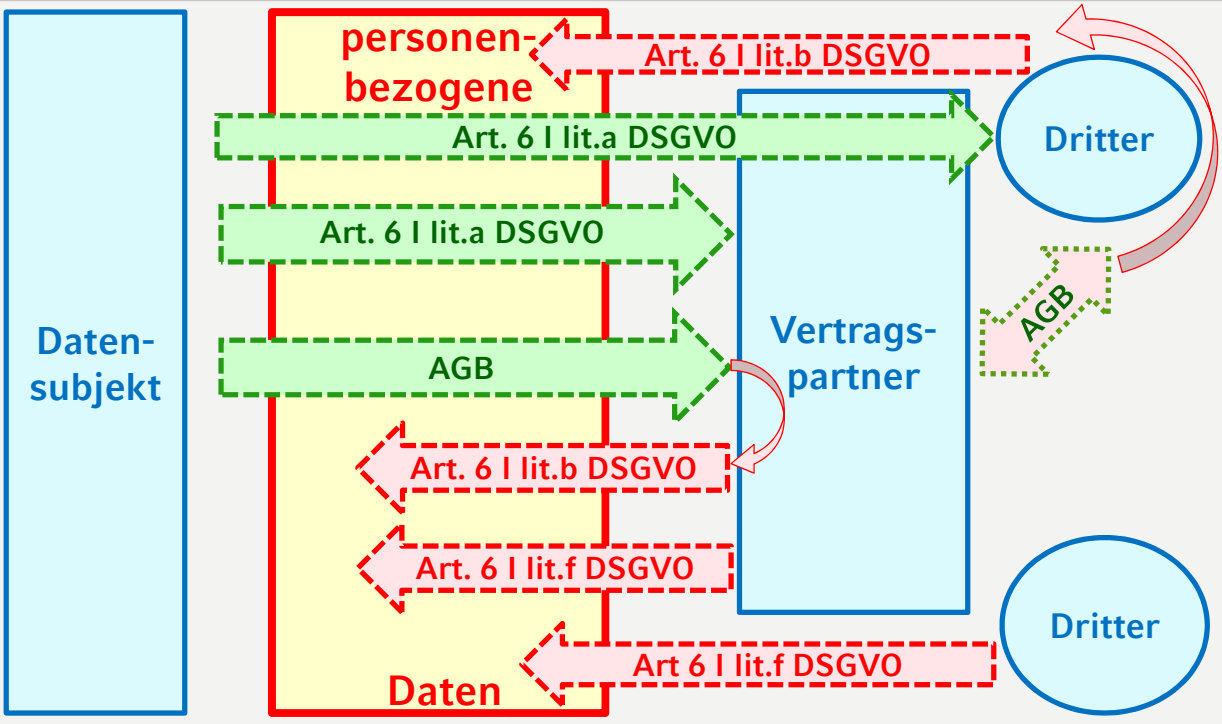
Art. 3 I 2: Anwendbar, soweit personenbezogene Daten über das Maß hinaus geleistet werden, das für die Vertragsdurchführung erforderlich ist.

Vertragsbeendigung

Art. 16 II: Es gilt die DS-GVO!
ErwG 40: Über die Folgen des Einwilligungswiderrufs entscheidet das nationale Vertragsrecht.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gestaltungsfragen
→ *personenbezogene Daten 4*



Einwilligung, Art. 6 I lit.a

1. Sog. Zweckbindung – Art. 6 I lit.a, IV / ErwG 39 S.6

2. Informationspflicht – Art. 4 Nr.11 / Art. 7 II S.2 / Art. 12 ff.

3. Freiwilligkeit – Kopplungsverbot, Art. 7 IV

4. Freie Widerruflichkeit – Art. 7 III
→ gegenüber dem Verantwortlichen
→ gegenüber bekannten/künftigen Datenverarbeitern
→ keine Disposition über die Widerruflichkeit

Folgen: Keine Klagbarkeit und keine Zwangsvollstreckung

Vertragsakzessorietät, Art. 6 I lit.b

1. Datensubjekt = Vertragspartei

2. Vertragserfüllung / Vorvertragliche Maßnahmen
→ Wer definiert die vertragliche Leistung?
→ Überschneidungen mit AGB-Kontrolle?
→ Datentreuhand- und Verwertungsvertrag?

3. Erforderlichkeit
→ Vermutung, dass anderweitiger wirtschaftlicher Zweck
(*von Westphalen/Wendehorst*)

Folge:
Nur anwendbar, soweit Daten gerade keine Gegenleistung sind.

Wahrung berechtigter Interessen, Art. 6 I lit.f

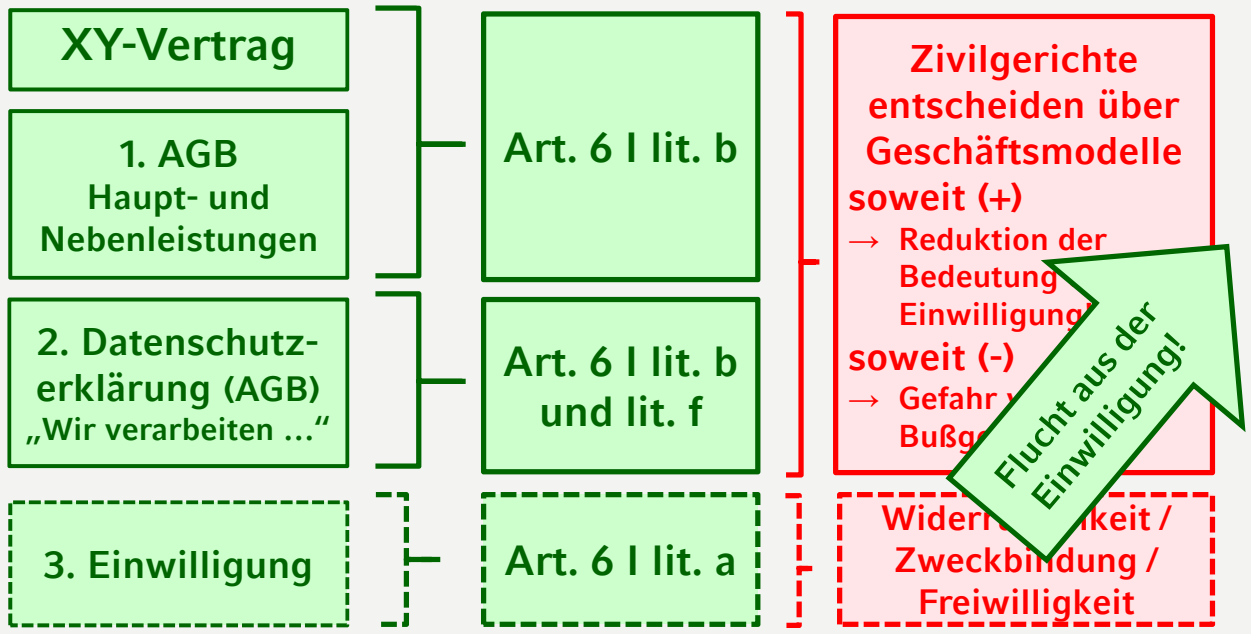
1. Berechtigte Interessen (Verantwortlicher oder Dritte)
   → kein Verstoß gegen die Grundsätze gemäß Art. 5
   → Direktwerbung (+), ErwG 47

2. Interessen/GrundR/Grundfreiheiten des Datensubjekts

3. Abwägung
   → kein Überwiegen von 2. gegenüber 1.

Widerspruchsrecht des Datensubjekts, Art. 21 I S.1
   → Ausnahme: Zwingend schutzwürdige Gründe für Verarbeitung

Folge:
Offene (Grund-)Rechts- und Interessenabwägung durch die nationalen Zivilgerichte der 28 Mitgliedstaaten.



Start: Art. 3 II DCDS-RL
Personenbezogen Daten, soweit nicht für Vertrag erforderlich

Art. 6 I lit.b DSGVO (-)	Art. 6 I lit.f DSGVO unwahrscheinlich	Art. 6 lit.a DSGVO (+)

Der Verantwortliche (ex ante) und die nationalen Gerichte (ex post) entscheiden auf Grundlage einer Abwägung aller berechtigten Interessen und der Grundrechte über die Zulässigkeit von Geschäftsmodellen.

1. **Freiwilligkeit**
   (OGH v. 31.08.2018 – 6 Ob 140/18h)
   Alternativangebot gegen Geld?
2. **Freie Widerruflichkeit**
   → Recht des Datensubjekts auf Vertragsfortsetzung gegen Geld?
   → Kündigungsrecht des Anbieters

Gliederung

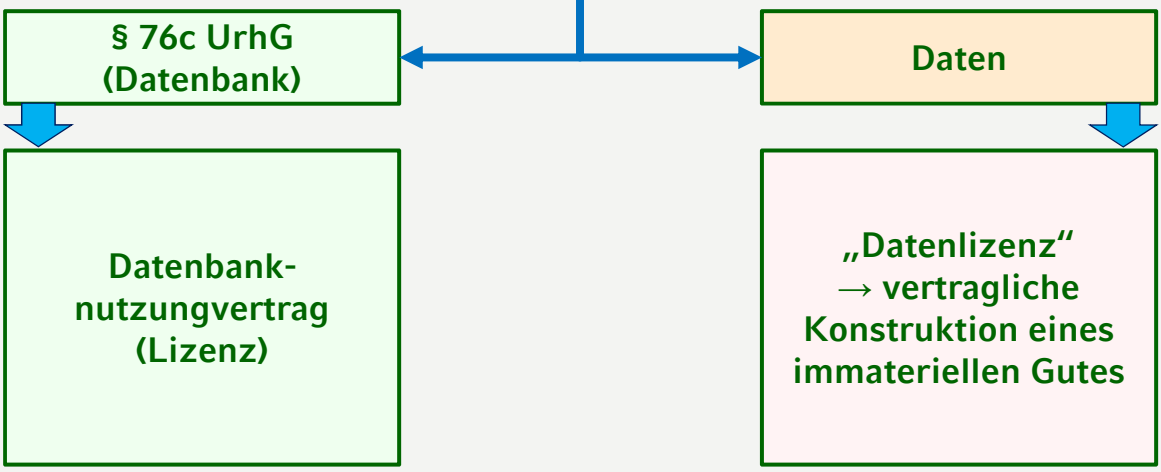
„Zahlen mit Daten“

Einräumung eines dauerhaften oder vorübergehenden Zugangs und Erlaubnis zur Nutzung der Daten, soweit diese über das vertraglich erforderliche Maß hinausgehen:

→ „Zahlen“ (-), wenn die Daten ausschließlich zur Erbringung von Diensten gegenüber Datenerzeuger gedient (predictive maintenance).

→ „Zahlen“ (+), wenn der Zugangs- und Nutzungsberechtigte die Daten für eigene Zwecke nutzen darf (Verbesserung eigener Produkte).

Datennutzungsvertrag



LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gestaltungsfragen
→ *maschinengenerierte Daten 3*

„Datenlizenz“

Sattler, in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0, 2019, Rn. 107 ff.

1. Technische und Organisatorische Schutzmaßnahmen
2. Vertraulichkeitsvereinbarung (NDA)

Folge: Vertragliches Verbot mit Erlaubnisvorbehalt

„Datenlizenz“
Vertragliche Konstruktion eines immateriellen Gutes

A. Klassifikation und Zuweisung der Daten an „Dateninhaber“
B. Definition/Einräumung von bestimmten Nutzungsrechten an den Daten und Datenergebnissen
C. Übergabe der Daten/Schnittstellendefinition/Datensicherheit
D. Service-Level-Agreement (Leistungsbeschreibung), ggfs. mit Pönalen
E. Vertragsbeendigung/Sublizenzen/Haftung/Daten-Escrow

EU-Kommission etabliert System der „überwachten“ Selbstregulierung und erwartet Standardklauseln bis 05/2020 (Art. 6 III DatenverkehrVO).

Dr. Andreas Sattler

Zentrum für Geistiges Eigentum, Medien- und Innovationsrecht
Donau-Universität Krems. Die Universität für Weiterbildung.

Text und Data Mining aus urheber- und datenschutzrechtlicher Sicht

Univ.-Prof. Ing. Dr. **Clemens Appl**, LL.M.

E-Mail: clemens.appl@donau-uni.ac.at
Tel: +43-2732-893-2411

www.donau-uni.ac.at/ip-center

CDSM-Richtlinie

Datenkorpus ist mehr als die Summe einzelner Daten

Text and Data Mining - Definitionen

- *A computational process whereby text or datasets are crawled by software that recognizes entities, relationships and actions.*

  The International Association of Scientific, Technical and Medical Publishers (2012)

- *The automated processing of digital materials, which may include texts, data, sounds, images or other elements, or a combination of these, in order to uncover new knowledge or insights.*

  Triaille (2014)

TDM - Charakteristika

- Automatisation
- Analytische Auswertung
- Digitaler Datenkorpus
- Zweck: Erkenntnisgewinn

Typischer Zugang von Nutzer/innen

Inhalte, die im Internet frei zugänglich sind, dürfen auch frei benützt werden.

Arbeitshypothese zum Ursprung dieses Zugangs:

- **Nutzer/innen sind gewohnt, digitale Inhalte im Internet frei zu konsumieren (Browsing, Caching, Streaming).**
- **Nutzer/innen sehen – mit Blick auf den Datenschutz – kein Schutzbedürfnis von Betroffenen, wenn diese ihre Daten freiwillig im Internet preisgeben.**
  - § 1 Abs 1 DSG 2000: *Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten,* ***soweit ein schutzwürdiges Interesse daran besteht***.

Access to Data

- Frei zugängliche Daten
  - „Frei“ = mit legalen (?) Mitteln (kostenlos?) zugänglich/abrufbar
  - Nutzungsbedingungen?
  - Gesetzliche Privilegierungen
- Open Data / Open Government Data
  - PSI-Richtlinie
  - Open Access Lizenzen
- Kommerziell verwertete Inhalte
  - One-to-many licensed – publizierte Inhalte
  - One-to-one licensed – vertrauliche Inhalte

Data Mining - Prozess

- **Datengewinnung**
- **Transformation**
- **Speicherung**
- **Auswertung**
- **Reporting**

1.

Urheberrechtliche Perspektive

Fokus: EU Copyright Reform
CDSM-Richtlinie

Urheberrechtliche Ausgangslage

- **Urheberrecht an einzelnen Daten**
  - Werkcharakter des jeweiligen Datums
  - Schutz von Werken und Werkteilen (§ 1 UrhG)
  - Kein Schutz an Ideen und Informationen: Dichotomie von Idee und Ausdrucksform
  - Niedrige Schutzschwelle: 11 Wörter können geschützt sein (EuGH C-5/08 – *Infopaq*); geringe Schwelle bei Fotografien (EuGH C-145/10 - *Painer*); aber kein Schutz für Einzelworte (OGH 4 Ob 96/97i - *Ramtha*)
- **Urheberrecht an Sammlungen und Datenbanken (§ 6; § 40f UrhG)**
  - Zusammenstellung von Daten manifestiert geistige Leistung in Bezug auf
    - Auswahl
    - Anordnung
  - Unabhängig vom Schutz einzelner Sammlungs- oder Datenbankelemente
- **Leistungsschutzrechte sowie Sui-generis-Schutz für Datenbanken**

Rechtfertigung von TDM aus urheberrechtlicher Sicht

- **TDM = Vervielfältigen (§15), Bearbeiten (§14 Abs 2; § 21), evtl Verbreitung (§ 16), Zurverfügungstellung (§18a)**

- **Lizenz**
  - Implizite Lizenz?
- **Freie Werknutzung**
  - § 41 UrhG - Amtsgebrauch
  - § 41a UrhG – flüchtige u begleitende Vervielfältigung
  - § 42 UrhG – Kopien zum eigenen oder privaten Gebrauch, insb **Forschung**
  - § 40h Abs 2 UrhG – Forschungsgebrauch von Datenbanken
  - S auch § 60d dUrhG und Sec 29A UK Copyright und Art 3 UDBM-RL-Entw jeweils mit ausdrücklichen Schranken zugunsten (wissenschaftlichem TDM)

- **Problemfelder:**
  - Kommerzielles (anwendungsorientiertes) TDM? Nur mit Lizenz?
  - Eingriff in Urheberpersönlichkeitsrecht?
  - Unterschiedliche Rechteinhaber auf verschiedenen Schutzebenen mit diverser Interessenlage

Fokus: Forschungsgebrauch in InfoSoc-RL und Datenbank-RL

- Art 9 lit b Datenbank-RL 96/9/EG: „***Entnahme*** *zur Veranschaulichung des Unterrichts oder* ***zu Zwecken der wissenschaftlichen Forschung****, sofern er die Quelle angibt und soweit dies durch den* ***nichtkommerziellen Zweck*** *gerechtfertigt ist*"

- Art 5 Abs 3 lit a InfoSoc-RL 2001/29/EG: „***Nutzung*** *ausschließlich zur Veranschaulichung im Unterricht oder* ***für Zwecke der wissenschaftlichen Forschung****, sofern - außer in Fällen, in denen sich dies als unmöglich erweist - die Quelle, einschließlich des Namens des Urhebers, wann immer dies möglich ist, angegeben wird und soweit dies zur Verfolgung* ***nicht kommerzieller Zwecke*** *gerechtfertigt ist*"

UK Copyright: Sec 29A CDPA (2014)
Copies for text and data analysis for non-commercial research

(1) The making of a copy of a work by a person who has **lawful access to the work** does not infringe copyright in the work provided that—

- (a)the copy is made in order that a person who has lawful access to the work may carry out a **computational analysis of anything recorded in the work** for the sole purpose of research for a **non-commercial purpose**, and
- (b)the copy is accompanied by a **sufficient acknowledgement** (unless this would be impossible for reasons of practicality or otherwise).

(2) Where a copy of a work has been made under this section, copyright in the work is infringed if—

- (a)the copy is transferred to any other person, except where the transfer is authorised by the copyright owner, or
- (b)the copy is used for any purpose other than that mentioned in subsection (1)(a), except where the use is authorised by the copyright owner.

(3) If a copy made under this section is subsequently dealt with—

- (a)it is to be treated as an infringing copy for the purposes of that dealing, and
- (b)if that dealing infringes copyright, it is to be treated as an infringing copy for all subsequent purposes.

(4) In subsection (3) "dealt with" means sold or let for hire, or offered or exposed for sale or hire.

(5) To the extent that a term of a **contract purports to prevent or restrict the making of a copy** which, by virtue of this section, would not infringe copyright, **that term is unenforceable.**

DE Urheberrecht: § 60d dUrhG
Text und Data Mining

(1) Um eine **Vielzahl von Werken** (Ursprungsmaterial) für die **wissenschaftliche Forschung** automatisiert auszuwerten, ist es zulässig,

1. das Ursprungsmaterial auch **automatisiert und systematisch zu vervielfältigen**, um daraus insbesondere durch **Normalisierung, Strukturierung und Kategorisierung** ein auszuwertendes Korpus zu erstellen, und
2. das Korpus einem bestimmt abgegrenzten Kreis von Personen für die gemeinsame wissenschaftliche Forschung sowie einzelnen Dritten zur Überprüfung der Qualität wissenschaftlicher Forschung öffentlich zugänglich zu machen.

Der Nutzer darf hierbei nur **nicht kommerzielle Zwecke** verfolgen.

(2) Werden Datenbankwerke nach Maßgabe des Absatzes 1 genutzt, so gilt dies als übliche Benutzung nach § 55a Satz 1. Werden unwesentliche Teile von Datenbanken nach Maßgabe des Absatzes 1 genutzt, so gilt dies mit der normalen Auswertung der Datenbank sowie mit den berechtigten Interessen des Datenbankherstellers im Sinne von § 87b Absatz 1 Satz 2 und § 87e als vereinbar.

(3) **Das Korpus und die Vervielfältigungen des Ursprungsmaterials sind nach Abschluss der Forschungsarbeiten zu löschen**; die öffentliche Zugänglichmachung ist zu beenden. Zulässig ist es jedoch, das Korpus und die Vervielfältigungen des Ursprungsmaterials den in den §§ 60e und 60f genannten **Institutionen zur dauerhaften Aufbewahrung zu übermitteln**.

Ausblick: CDSM-RL

- Definition von **Text and Data Mining** in Art 2 Abs 2:
  - „Text und Data Mining" bezeichnet eine **Technik für die automatisierte Analyse von Texten und Daten in digitaler Form**, mit deren Hilfe Informationen unter anderem – aber nicht ausschließlich – über Muster, Trends und Korrelationen gewonnen werden können.
  - **Texte und Daten?**
    ErwGr 8: „... *Texte, Töne, Bilder und Daten ...*" – Gegenstand bleibt vage

- **CDSM-RL privilegiert TDM**
  - generell (Art 4) und
  - speziell zugunsten von Forschungs-und Kulturerbeeinrichtungen (Art 3)
    s bereits COM(2016)0593

Ausblick: Generelles TDM-Privileg nach Art 4

- **Begünstigte:** Jedermann

- **Privilegierung von Vervielfältigung und Entnahme**
  - **Zwecke des TDM**
  - **rechtmäßig zugängliche Quelle**

- **Speicherdauer:** Datenkorpus darf nur solange aufbewahrt werden, wie es der TDM Zweck erfordert.
  - Verhältnis zu bestehenden freien Werknutzungen?

Ausblick: Generelles TDM-Privileg nach Art 4

- **Vorbehalt durch Rechteinhaber möglich** (Art 4 Abs 3, Art 7 Abs 1 e contrario)
  - „*ausdrücklich in angemessener Weise*"
  - zB maschinenlesbare Hinweise bei Internetpublikationen geboten; dies gilt auch für Metadaten oder AGB (ErWGr 18)

- **iE: Zweifelsregelung, wonach frei zugängliche Inhalte frei benutzt werden dürfen**

- **Kein Vergütungsanspruch?**
  - ErwGr 17 gilt mE nur für Art 3
  - Vereinbarkeit mit Dreistufentest?

Ausblick: Spezielles TDM-Privileg nach Art 3

- **Begünstigte:**
  - **Forschungsorganisation** (Art 2 Abs 1)
    - Hochschulen inkl deren Bibliotheken, Forschungsinstitute oder andere Einrichtungen mit „vorrangigem Ziel" der wissenschaftlichen Forschung *oder* der Lehre
    - nicht gewinnorientiert (oder Re-Investieren von Gewinnen in Forschung) oder in einem „*anerkannten Auftrag im öffentlichen Interesse*" tätig
    - Kein Unternehmen darf bevorzugten Zugang zu den Ergebnissen erhalten.
  - **Kulturerbeeinrichtung** (Art 2 Abs 3)
    - öffentlich zugängliche Bibliothek oder Museum, Archiv

- **Privilegierung von Vervielfältigung und Entnahme**
  - **Zwecke des TDM im Rahmen wissenschaftlicher Forschung**
    - ErwGr 12: Natur- und Geisteswissenschaft
  - **rechtmäßiger Zugang**
    - ErwGr 14: Open Access, lizenzierte Inhalte oder „*andere rechtmäßige Mittel*" zugänglich; „*im Internet frei verfügbare Inhalte*"?

Ausblick: Spezielles TDM-Privileg nach Art 3

- **Speicherdauer:** Wissenschaftlicher Zweck (inkl Qualitätssicherung) bestimmt Dauer; Speicherung muss mit „angemessenen Sicherheitsvorkehrungen" einhergehen.
- **Rechteinhaber haben Recht auf Sicherung der Sicherheit und Integrität der Datenbanken und Netze (Art 3 Abs 3)**
  - Verhältnismäßigkeit!
- **Keine Vergütungspflicht?**
  - ErwGr 17
- **Stakeholder-Dialog** zu Speicherung (Abs 2) und Sicherheit (Abs 3)
  - MS wirken auf einvernehmliche Festlegungen hin …

Bewertung der Neuregelungen

- **Artt 3 und 4 sind verpflichtend umzusetzen.**
- **Generelles TDM-Privileg ist eine Zweifelsregelung** dahin, dass frei zugängliche Inhalte grds ausgewertet werden dürfen. Rechteinhaber müssen daher in Zukunft „*ausdrücklich in angemessener Weise*" TDM Vorbehalte offenlegen.
- **Spezielles TDM-Privileg begünstigt nur Forschungs- und Kulturerbeeinrichtungen,** hat zwingenden Charakter und ist vergütungsfrei. Rechteinhaber dürfen Datenbanken und Netze gegen (technisch) unzumutbare Nutzungen absichern.
- Artt 3 und 4 enthalten **keine Regelung betreffend Urheberpersönlichkeitsrechte, Bearbeitungen oder Ergebnisverwertung**

2.

Datenschutzrechtliche Perspektive

Überblick am
Beispiel Social Media

Datenschutzrechtliche Ausgangslage am Beispiel „Social Media Posting“

- Datenschutz für personenbezogene Daten, durch die eine (lebende natürliche) Person direkt oder indirekt identifizierbar ist.
  - Social Media Postings sind mE personenbezogene Daten, weil diese regelmäßig einen Bezug zum jeweiliger Verfasser aufweisen.
  - Der Personenbezug von Postings lässt sich idR nicht durch weglassen des Verfassers „anonymisieren“, weil Postings mit einfachsten (legalen) Mitteln re-identifiziert werden können.
- Es gilt der datenschutzrechtliche Verbotsgrundsatz, sodass die Verarbeitung einer Rechtfertigung bedarf, also „**rechtmäßig**“ iSd Art 5 Abs 1 lit a iVm Artt 6, 9 DSGVO erfolgen muss.
- Problem: **Zweckänderung** (Art 5 Abs 1 lit b DSGVO)
  - Der Verfasser eines Postings hat dieses zu bestimmten **Zweck** auf der Social Media Plattform veröffentlicht: Plattform soll Posting einem definiertem Publikum zugänglich zu machen; damit ist implizit weiterhin davon auszugehen, dass das Publikum das Posting „zur Kenntnisnehmen“ und ggf „Teilen darf“.
  - Eine Nutzung durch das Publikum über typische Social Media Funktionen hinaus liegt mE jenseits des vom Verfassers angestrebten Zwecks.

Rechtfertigung von TDM aus datenschutzrechtlicher Sicht

- **Verbotsgrundsatz:** Keine Verarbeitung personenbezogener Daten ohne Legitimation gemäß DSGVO

- Rechtmäßigkeit durch Einwilligung (Art 6 Abs 1 lit a DSGVO) oder gesetzliche Grundlage (Art 6 Abs 1 lit b ff DSGVO)
- Anwendung von Forschungsprivilegien (Art 5 Abs 1 lit b DSGVO bzgl Zweckänderung; Art 14 Abs 5 lit b DSGVO bzgl Auskunftserteilung)

- Postings „abgreifen“ von Social Media Plattformen
  - Datenerhebung nicht beim Betroffenen (Art 14 DSGVO)
  - Zweckänderung durch Auswertung
  - Reichweite der Zustimmung?
- **Speicherung und Speicherdauer?**

3.

Zusammenfassung

Conclusio

- **Aus dem freien Zugang zu Daten folgt nicht automatisch deren freie – konsenslose – Folgeverwertung im Rahmen von TDM.**
- Bei der Bewertung der Zulässigkeit sind **Urheberrecht** (allenfalls Knowhow-Schutz) einerseits und **Datenschutzrecht** andererseits zu prüfen.
- „**Anwendungsorientiertes (kommerzielles) TDM**" genießt mE keine besonderen urheberrechtlichen oder datenschutzrechtlichen Privilegierungen
  - Änderung durch CDSM-RL (Zweifelsregelung) bringt Rechtssicherheit, sorgfältige Prüfung der Datenquellen bleibt aber erforderlich
- „**Wissenschaftliches TDM**" genießt bestimmte urheberrechtliche und datenschutzrechtliche Privilegien.

Policy Implications

- **Urheberrecht ist kein Informationsschutz**
  - Extraktion von Information aus urheberrechtlichen geschützten Werken liegt grds jenseits des Schutzbereichs.
  - Geltendes Urheberrecht unterscheidet hier aber (unsachlich?) zwischen analoger (zB Lesen und Verarbeiten) und digitaler Extraktion (zB ADV-Auswertung, die ohne Kopieren der Rohdaten nicht auskommt)
- **Mangelhafte Kohärenz von Urheberrecht und Datenschutz bzgl TDM**
  - DSGVO adressiert TDM nicht ausdrücklich;
  - Einheitliche Auslegung von Wissenschaft und Forschung?
- **Wissenschaftsethik?**

Zentrum für Geistiges Eigentum, Medien- und Innovationsrecht
Donau-Universität Krems. Die Universität für Weiterbildung.

Text und Data Mining aus urheber- und datenschutzrechtlicher Sicht

Univ.-Prof. Ing. Dr. **Clemens Appl**, LL.M.

E-Mail: clemens.appl@donau-uni.ac.at
Tel: +43-2732-893-2411

www.donau-uni.ac.at/ip-center

Auszug CDSM-RL

P8_TA-PROV(2019)0231
Urheberrecht im digitalen Binnenmarkt

[…]

(8) Mit neuen, im Allgemeinen als Text und Data Mining bekannten Verfahren können in digitaler Form vorliegende Informationen wie Texte, Töne, Bilder oder Daten mit Computern automatisch ausgewertet werden. Mittels Text und Data Mining lassen sich große Informationsmengen verarbeiten, um neue Erkenntnisse zu gewinnen und neue Trends zu erkennen. Das Text und Data Mining ist die vorherrschende Technik in der Digitalwirtschaft, doch besteht weitgehend Einvernehmen darüber, dass diese Technik vor allem für die Forschung von besonderem Nutzen ist und damit auch Innovationen gefördert werden. Von Nutzen ist diese Technik zudem für Hochschulen und andere Forschungsorganisationen sowie für Einrichtungen des Kulturerbes, da diese möglicherweise ebenfalls Forschung im Zusammenhang mit ihrer hauptsächlichen Tätigkeit betreiben könnten. In der Union sehen sich derartige Organisationen und Einrichtungen allerdings damit konfrontiert, dass hinsichtlich des möglichen Umfangs des Text und Data Mining von Inhalten Rechtsunsicherheit herrscht. Mitunter kann das Text und Data Mining Handlungen umfassen, die durch das Urheberrecht, das Sui-generis-Recht an Datenbanken oder beides geschützt sind, vor allem wenn es um die Vervielfältigung von Werken oder sonstigen Schutzgegenständen, die Entnahme von Inhalten aus einer Datenbank oder beides geht, also Handlungen, die beispielsweise erfolgen, wenn die Daten während des Vorgangs des Text und Data Mining normalisiert werden. Können keine Ausnahmen oder Beschränkungen geltend gemacht werden, so ist für solche Handlungen die Erlaubnis des Rechteinhabers erforderlich.

(9) Das Text und Data Mining kann auch für reine, nicht urheberrechtlich geschützte Fakten oder Daten erfolgen, und in diesen Fällen ist nach dem Urheberrecht keine Erlaubnis erforderlich. Es kann auch Fälle des Text und Data Mining geben, in denen keine Vervielfältigungshandlung erfolgt oder die Vervielfältigungen unter die in Artikel 5 Absatz 1 der Richtlinie 2001/29/EG vorgesehene verbindliche Ausnahme für vorübergehende Vervielfältigungshandlungen fallen, die auch künftig auf Verfahren des Text und Data Mining angewandt werden sollte, die nicht die Anfertigung von Kopien in einem über diese Ausnahme hinausgehenden Umfang einschließen.

(10) Das Unionsrecht sieht bestimmte Ausnahmen und Beschränkungen für die Nutzung zu Zwecken der wissenschaftlichen Forschung vor, die auf Handlungen des Text und Data Mining angewandt werden können. Diese Ausnahmen und Beschränkungen sind jedoch fakultativ und noch nicht vollständig an die Techniken in der wissenschaftlichen Forschung angepasst. Zudem könnten die Lizenzbedingungen in den Fällen, in denen Forscher rechtmäßig Zugang zu Inhalten haben, etwa durch das Abonnieren von Veröffentlichungen oder durch Lizenzen für den offenen Zugang, einen Ausschluss von des Text und Data Mining vorsehen. Da die Unterstützung durch die Digitaltechnik in der Forschung immer wichtiger wird, besteht die Gefahr, dass die Wettbewerbsposition der Union in der Forschung hiervon beeinträchtigt wird, wenn die Rechtsunsicherheit im Hinblick auf Text und Data Mining nicht beseitigt wird.

(11) Die Rechtsunsicherheit im Hinblick auf Text und Data Mining sollte beseitigt werden, indem für Hochschulen und andere Forschungsorganisationen sowie für Einrichtungen des Kulturerbes eine verbindliche Ausnahme für das ausschließliche Recht auf Vervielfältigung, aber auch auf das Recht, Entnahmen aus einer Datenbank zu untersagen, eingeführt wird. Im Einklang mit der derzeitigen Forschungspolitik der Union, die Hochschulen und Forschungsinstitute zur Zusammenarbeit mit der Privatwirtschaft anhält, sollten auch Forschungsorganisationen eine solche Ausnahme nutzen dürfen, sofern ihre Forschungstätigkeit im Rahmen öffentlichprivater Partnerschaften durchgeführt wird. Forschungsorganisationen und Einrichtungen des Kulturerbes sollten auch künftig zu den Begünstigten der Ausnahmeregelung zählen, sich aber bei der Durchführung des Text und Data Mining auch ihrer privaten Partner bedienen können, einschließlich unter Nutzung ihrer technischen Werkzeuge.

(12) In der Union gibt es eine Vielzahl von Forschungsorganisationen, deren vorrangiges Ziel die wissenschaftliche Forschung oder die Forschung und Lehre ist. Im Sinne dieser Richtlinie bezieht sich der Ausdruck „wissenschaftliche Forschung“ sowohl auf die Naturwissenschaften als auch auf die Geisteswissenschaften. Angesichts der Vielfalt dieser Einrichtungen sollte Einvernehmen darüber erzielt werden, was als Forschungsorganisation gilt. Beispielsweise sollten zusätzlich zu Universitäten und anderen Hochschuleinrichtungen und ihren Bibliotheken auch Einrichtungen wie Forschungsinstitute und Forschungskliniken darunter fallen. Trotz unterschiedlicher Rechtsformen und Strukturen ist den Forschungsorganisationen in den Mitgliedstaaten in der Regel gemein, dass sie entweder nicht gewinnorientiert sind oder in staatlich anerkanntem Auftrag im öffentlichen Interesse

handeln. Kennzeichnend für einen solchen Auftrag im öffentlichen Interesse könnten beispielsweise die Finanzierung durch die öffentliche Hand oder Bestimmungen im nationalen Recht oder öffentlichen Verträgen sein. Hingegen sollten für die Zwecke dieser Richtlinie Organisationen nicht als Forschungsorganisationen gelten, wenn solche Organisationen dem bestimmenden Einfluss gewerblicher Unternehmen unterliegen, die aufgrund der strukturellen Gegebenheiten beispielsweise in ihrer Eigenschaft als Anteilseigner oder Mitglieder Kontrolle ausüben können und dadurch einen bevorzugten Zugang zu den Forschungsergebnissen erhalten könnten.

(13) Als Einrichtungen des kulturellen Erbes sollten öffentlich zugängliche Bibliotheken und Museen unabhängig von der Art der dauerhaft in ihren Sammlungen befindlichen Werke oder sonstigen Schutzgegenstände sowie Archive und im Bereich des Film- oder Tonerbes tätige Einrichtungen gelten. Als solche sollten unter anderem auch Nationalbibliotheken und Nationalarchive gelten sowie die Archive und die öffentlich zugänglichen Bibliotheken von Bildungseinrichtungen, Forschungsorganisationen und öffentlich-rechtlichen Rundfunkanstalten.

(14) Forschungsorganisationen und Einrichtungen des kulturellen Erbes einschließlich der ihnen angehörenden Personen sollten unter die Ausnahme für das Text und Data Mining fallen, was die Inhalte betrifft, zu denen sie rechtmäßig Zugang haben. Als rechtmäßiger Zugang sollte der Zugang zu Inhalten auf der Grundlage einer Open Access Strategie oder durch vertragliche Vereinbarungen zwischen Rechteinhabern und Forschungsorganisationen bzw. Einrichtungen des Kulturerbes, etwa durch Abonnements, oder durch andere rechtmäßige Mittel gelten. So sollten beispielsweise im Fall von Abonnements durch Forschungsorganisationen oder Einrichtungen des Kulturerbes die ihnen angehörenden und das Abonnement nutzenden Personen als Personen mit rechtmäßigem Zugang gelten. Als rechtmäßiger Zugang sollte auch der Zugang zu im Internet frei verfügbaren Inhalten gelten.

(15) In bestimmten Fällen, etwa zur anschließenden Überprüfung der Ergebnisse wissenschaftlicher Forschung, könnte es erforderlich sein, dass Forschungsorganisationen und Einrichtungen des Kulturerbes die im Rahmen der Ausnahme zum Zwecke der Durchführung eines Text und Data Mining angefertigten Kopien aufbewahren. In diesen Fällen sollten die Kopien in einer sicheren Umgebung gespeichert werden. Den Mitgliedstaaten sollte es freigestellt sein, auf nationaler Ebene und nach Diskussionen mit den einschlägigen Interessenträgern weitere spezifische Regelungen für die Aufbewahrung der Kopien festlegen, darunter auch die Fähigkeit, zum Zwecke der Speicherung derartiger Kopien vertrauenswürdige Stellen zu benennen. Damit die Inanspruchnahme der Ausnahme nicht ungebührlich eingeschränkt wird, sollten diese Regelungen verhältnismäßig und darauf beschränkt sein, was für die sichere Aufbewahrung der Kopien und die Verhinderung der unbefugten Nutzung erforderlich ist. Die Nutzung zum Zwecke der wissenschaftlichen Forschung außerhalb des Text und Data Mining, etwa die Begutachtung unter wissenschaftlichen Fachkollegen und gemeinsame Forschungsarbeiten, sollte nach wie vor unter die Ausnahme oder Beschränkung im Sinne von Artikel 5 Absatz 3 Buchstabe a der Richtlinie 2001/29/EG fallen, sofern diese Bestimmung anwendbar ist.

(16) Im Hinblick auf eine große Anzahl von Zugangs- und Download-Anfragen für ihre Werke oder sonstige Schutzgegenstände sollten die Rechteinhaber Maßnahmen treffen dürfen, wenn die Sicherheit und Integrität ihrer Systeme oder Datenbanken gefährdet sein könnte. Mit solchen Maßnahmen könnte beispielsweise sichergestellt werden, dass nur Personen mit rechtmäßigem Zugang zu den Daten der Rechteinhaber auf diese Daten zugreifen können, auch mittels Überprüfung von IP-Adressen oder Nutzerauthentifizierung. Solche Maßnahmen sollten im Hinblick auf die diesbezüglichen Risiken verhältnismäßig bleiben und nicht über das zur Verwirklichung des Ziels – d. h. die Wahrung der Sicherheit und Integrität des Systems – notwendige Maß hinausgehen, und der wirksamen Anwendung der Ausnahme nicht entgegenstehen.

(17) In Anbetracht der Art und des Umfangs der Ausnahme, die auf Einrichtungen beschränkt ist, die wissenschaftliche Forschung betreiben, würde der den Rechteinhabern im Zuge dieser Ausnahme möglicherweise entstehende Schaden minimal sein. Daher sollten die Mitgliedstaaten keinen Ausgleich für Rechteinhaber bei Nutzungen im Rahmen der mit dieser Richtlinie eingeführten Ausnahmen für das Text und Data Mining vorsehen.

(18) Verfahren des Text und Data Mining haben nicht nur im Zusammenhang mit der wissenschaftlichen Forschung hohe Bedeutung, sondern sie werden auch in großem Umfang sowohl von privaten als auch öffentlichen Einrichtungen eingesetzt, um große Datenmengen in verschiedenen Lebensbereichen und zu unterschiedlichen Zwecken zu analysieren, auch für staatliche Dienste, komplexe unternehmerische Entscheidungen und die Entwicklung neuer Anwendungen oder Technologien. Die Rechteinhaber sollten auch künftig Lizenzen für die Nutzung ihrer Werke oder sonstigen Schutzgegenstände erteilen können, die weder unter die in dieser Richtlinie vorgesehene verbindliche Ausnahme für Text und Data Mining zum Zwecke der wissenschaftlichen Forschung noch unter die gemäß der Richtlinie 2001/29/EG geltenden Ausnahmen und Beschränkungen fallen. Gleichzeitig sollte berücksichtigt werden, dass die Nutzer des Text

und Data Mining mit Rechtsunsicherheit hinsichtlich der Frage konfrontiert sein könnten, ob Vervielfältigungen und Entnahmen zum Zwecke des Text und Data Mining bei rechtmäßigem Zugang zu Werken oder sonstigen Schutzgegenständen vorgenommen werden dürfen, insbesondere wenn bei den zum Zwecke der Durchführung des technischen Vorgangs vorgenommenen Vervielfältigungen und Entnahmen möglicherweise nicht alle Bedingungen der für vorübergehende Vervielfältigungshandlungen in Artikel 5 Absatz 1 der Richtlinie 2001/29/EG vorgesehenen Ausnahme erfüllt sind. Um in diesen Fällen für mehr Rechtssicherheit zu sorgen und auch in der Privatwirtschaft zu Innovationen anzuregen, sollte diese Richtlinie unter bestimmten Bedingungen eine Ausnahme oder Beschränkung für Vervielfältigungen und Entnahmen von Werken oder sonstigen Schutzgegenständen für die Zwecke des Text und Data Mining vorsehen und es ermöglichen, dass die angefertigten Kopien so lange wie zum Zwecke dieses Text und Data Mining erforderlich aufbewahrt werden. Diese Ausnahme oder Beschränkung sollte nur gelten, wenn der Begünstigte rechtmäßigen Zugang zu dem Werk oder sonstigen Schutzgegenstand hat, wozu auch gehört, dass es bzw. er der Öffentlichkeit im Internet zugänglich gemacht wurde, und soweit die Rechteinhaber sich nicht in angemessener Weise das Recht, Vervielfältigungen und Entnahmen zum Zwecke des Text und Data Mining anzufertigen, vorbehalten haben. Wurden Inhalte im Internet öffentlich zugänglich gemacht, so sollte es als angemessen erachtet werden, einen Rechtsvorbehalt mit maschinenlesbaren Mitteln auszusprechen; Das gilt auch für Metadaten und Geschäftsbedingungen einer Website oder eines Dienstes. Andere Nutzungen sollten von dem Rechtsvorbehalt für die Zwecke des Text und Data Mining nicht betroffen sein. In anderen Fällen kann es angemessen sein, einen Rechtsvorbehalt mit anderen Mitteln, etwa in vertraglichen Vereinbarungen oder durch eine einseitige Erklärung, auszusprechen. Die Rechteinhaber sollten in der Lage sein, Maßnahmen zu treffen, mit denen sie sicherstellen, dass ihre diesbezüglichen Vorbehalte Beachtung finden. Diese Ausnahme oder Beschränkung sollte die in dieser Richtlinie niedergelegte verbindliche Ausnahme für das Text und Data Mining zu wissenschaftlichen Forschungszwecken sowie die in Artikel 5 Absatz 1 der Richtlinie 2001/29/EG vorgesehene Ausnahme für vorübergehende Vervielfältigungshandlungen unberührt lassen.

[…]

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Richtlinie gelten folgende Begriffsbestimmungen:

1. „Forschungsorganisation“ bezeichnet eine Hochschule einschließlich ihrer Bibliotheken, ein Forschungsinstitut oder eine sonstige Einrichtung, deren vorrangiges Ziel die wissenschaftliche Forschung oder die Lehrtätigkeit – auch in Verbindung mit wissenschaftlicher Forschung – ist, die

a) in ihrer Tätigkeit nicht gewinnorientiert ist oder alle Gewinne in ihre wissenschaftliche Forschung reinvestiert, oder

b) im Rahmen eines von einem Mitgliedstaat anerkannten Auftrags im öffentlichen Interesse tätig ist, wobei kein Unternehmen, das einen bestimmenden Einfluss auf diese Organisation hat, bevorzugten Zugang zu den Ergebnissen der wissenschaftlichen Forschung erhält.

2. „Text und Data Mining“ bezeichnet eine Technik für die automatisierte Analyse von Texten und Daten in digitaler Form, mit deren Hilfe Informationen unter anderem – aber nicht ausschließlich – über Muster, Trends und Korrelationen gewonnen werden können.

3. „Einrichtung des Kulturerbes“ bezeichnet eine öffentlich zugängliche Bibliothek oder Museum, Archiv oder eine im Bereich des Film- oder Tonerbes tätige Einrichtung.

[…]

Artikel 3
Text und Data Mining zum Zwecke der wissenschaftlichen Forschung

(1) Die Mitgliedstaaten sehen eine Ausnahme von den in Artikel 5 Buchstabe a und Artikel 7 Absatz 1 der Richtlinie 96/9/EG, Artikel 2 der Richtlinie 2001/29/EG, und Artikel 15 Absatz 1 der vorliegenden Richtlinie festgelegten Rechten für Vervielfältigungen und Entnahmen vor, die durch Forschungsorganisationen und Einrichtungen des Kulturerbes von Werken oder sonstigen Schutzgegenständen, zu denen sie rechtmäßig Zugang haben, zum Zwecke der wissenschaftlichen Forschung für die Text und Data Mining vorgenommen werden.

(2) Vervielfältigungen und Entnahmen von Werken oder sonstigen Schutzgegenständen, die gemäß Absatz 1 angefertigt wurden, sind mit angemessenen Sicherheitsvorkehrungen zu speichern und dürfen zum Zwecke der wissenschaftlichen Forschung, auch zur Überprüfung wissenschaftlicher Erkenntnisse, aufbewahrt werden.

(3) Die Rechteinhaber müssen Maßnahmen durchführen können, um die Sicherheit und Integrität der Netze und Datenbanken zu wahren, in denen die Werke oder sonstigen Schutzgegenstände gespeichert sind. Diese Maßnahmen dürfen über das für die Verwirklichung dieses Ziels Notwendige nicht hinausgehen.

(4). Die Mitgliedstaaten wirken darauf hin, dass Rechteinhaber, Forschungsorganisationen und

Einrichtungen des Kulturerbes einvernehmlich bewährte Vorgehensweisen bei der die Umsetzung der in Absatz 2 genannten Verpflichtung bzw. die Durchführung der in Absatz 3 genannten Maßnahmen definieren.

Artikel 4
Ausnahmen und Beschränkungen für das Text und Data Mining

(1) Für zum Zwecke des Text und Data Mining vorgenommene Vervielfältigungen und Entnahmen von rechtmäßig zugänglichen Werken und sonstigen Schutzgegenständen sehen die Mitgliedstaaten eine Ausnahme oder Beschränkung von den Rechten vor, die in Artikel 5 Buchstabe a und Artikel 7 Absatz 1 der Richtlinie 96/9/EG, Artikel 2 der Richtlinie 2001/29/EG, Artikel 4 Absatz 1 Buchstaben a und b der Richtlinie 2009/24/EG und Artikel 15 Absatz 1 der vorliegenden Richtlinie niedergelegt sind.
(2) Vervielfältigungen und Entnahmen nach Absatz 1 dürfen so lange aufbewahrt werden, wie es für die Zwecke des Text und Data Mining notwendig ist.
(3) Die Ausnahmen und Beschränkungen nach Absatz 1 finden Anwendung, sofern die jeweiligen Rechteinhaber die in Absatz 1 genannten Werke und sonstigen Schutzgegenstände nicht ausdrücklich in angemessener Weise, etwa mit maschinenlesbaren Mitteln im Fall von online veröffentlichten Inhalten, mit einem Nutzungsvorbehalt versehen haben.
(4) Dieser Artikel lässt die Anwendung von Artikel 3 unberührt.

[…]

Artikel 7
Gemeinsame Bestimmungen

(1) Vertragsbestimmungen, die den in den Artikeln 3, 5 und 6 festgelegten Ausnahmen zuwiderlaufen, sind nicht durchsetzbar.
(2) Artikel 5 Absatz 5 der Richtlinie 2001/29/EG findet auf die unter diesem Titel genannten Ausnahmen und Beschränkungen Anwendung. Artikel 6 Absatz 4 Unterabsatz 1, 3 und 5 der Richtlinie 2001/29/EG finden auf die Artikel 3 bis 6 der vorliegenden Richtlinie Anwendung.

INFOLAW
WWW.INFOLAW.AT

PERSONENFOTOS AUS PERSÖNLICHKEITS- UND DATENSCHUTZRECHTLICHER SICHT

13. IT-Rechtstag

23.5.2019

Andreas Seling & Dominik Schelling

DORDA

WIR SCHAFFEN KLARHEIT.

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Agenda

1. Einleitung
2. Verhältnis Persönlichkeitsschutz vs Datenschutz
3. Rechtsgrundlagen
4. Ausgewählte Praxisfälle
5. Wesentliche Rechte der Abgebildeten
6. Fazit

1. Einleitung

Ausgangspunkt

1. Einleitung

Entwicklung der Rechtslage rund um Bildaufnahmen

Bislang

- Zivilrechtlicher Bildnisschutz
- Praktisch große Bedeutung, viele Judikate
- Datenschutzrechtliche Aspekte: bislang kaum praktische Rolle
- Obwohl: Bild einer Person = personenbezogenes Datum

Seit 25.5.2018 - DSGVO

- Weiterhin Qualifikation als personenbezogenes Datum
- Jedoch: höheres Bewusstsein und neuer Sanktionsmechanismus

➔ Verschiebung des Fokus

1. Einleitung

Allgemeines Regelungsregime – Urheberrecht

Bildnisschutz

- § 78 UrhG "Recht am eigenen Bild" (1936)
- Materiell: Persönlichkeitsrecht
- Regelt öffentliche Ausstellung und Verbreitung von Personenbildnissen
- Bildnisaufnahme: OGH "*Zur Belustigung*" (6 Ob 256/12h)
- Grundsatz der Verwendungsfreiheit ("*ja, aber*")

"Bildnisse von **Personen** dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, **verbreitet** werden, wenn dadurch **berechtigte Interessen** des Abgebildeten […] verletzt würden."

1. Einleitung

Allgemeines Regelungsregime – Datenschutzrecht

Bild als personenbezogenes Datum

- idR keine besonderen Kategorien pb Daten (ErwGr 51 DSGVO)
- Aufnahme und Verwendung von Personenfotos = Datenverarbeitung
- Rechtsgrundlage erforderlich (Art 6 DSGVO)
  - Sonderbestimmungen zur "*Bildaufnahme*" in § 12 und 13 DSG
    - idR Einwilligung oder berechtigtes Interesse
    - besondere Sicherheitsmaßnahmen und Kennzeichnungspflichten
- Informationspflichten nach Art 12 ff DSGVO und Rechte der Betroffenen nach Art 15 ff DSGVO greifen
- Ausnahmen vom Anwendungsbereich:
  - Haushaltsausnahme (Art 2 Abs 2 lit c DSGVO)
  - Medienprivileg – jedoch nicht schrankenlos (§ 9 DSG iVm Art 85 DSGVO)

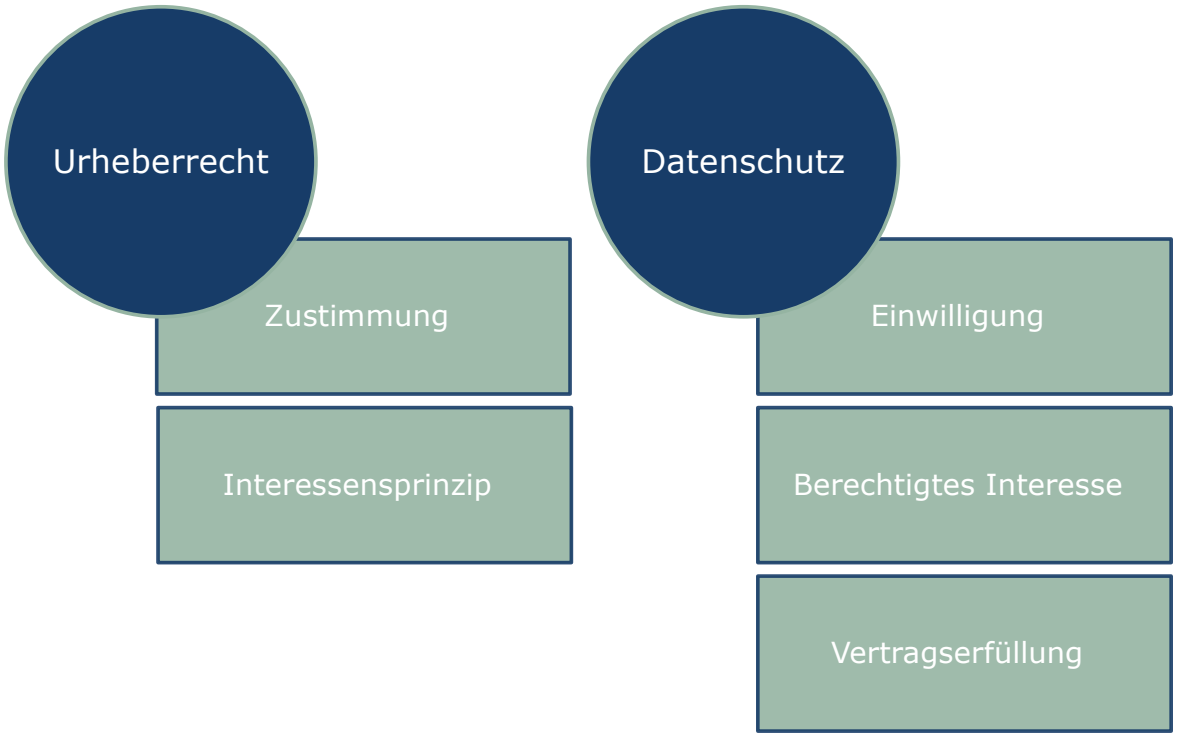
2. Verhältnis Urheberrecht vs Datenschutz

- Grundsatz: Anwendungsvorrang des Unionsrechts vor entgegenstehendem nationalen Recht
  - Kein Widerspruch UrhG vs DSGVO
    - Unterschiedliche Anwendungsbereiche
    - Unterschiedliche Zwecke und Ziele
    - Unterschiedliche Ansprüche
- OLG Köln, 18.6.2018, 15 W 27/18 und 8.10.2018, 15 U 110/18:
  - Jedenfalls im journalistischen Bereich schließt die DSGVO die Anwendung des KUG nicht aus

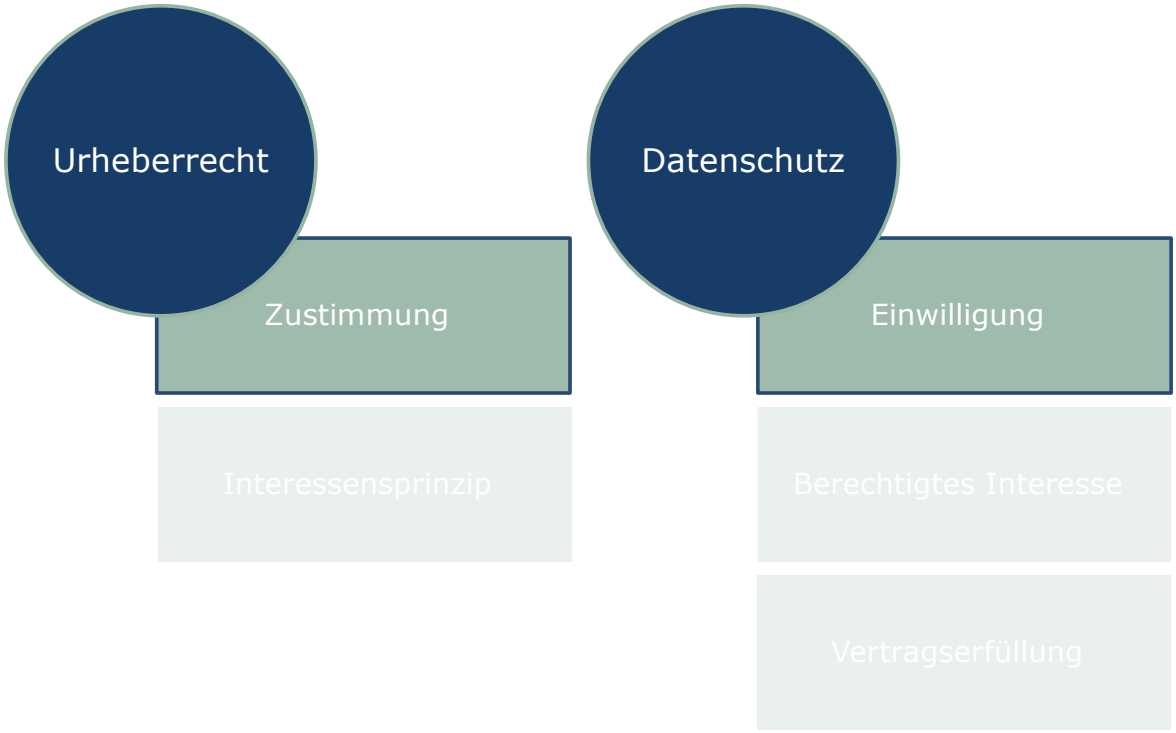
➔ uE idR beide Regime und Ansprüche aus beiden Materien zu berücksichtigen

➔ häufig parallele Wertungen

3. Rechtsgrundlagen



3. Rechtsgrundlagen



3. Rechtsgrundlagen – Urheberrecht

Zustimmung

- Kein Bildnisschutz, wenn Abgebildeter Veröffentlichung zustimmt
- keine Anforderungen an die Form
- kann auch schlüssig erteilt werden
  - zB Model für Berufsfotograf (4 Ob 18/94 – *Leiden für die Schönheit*)
- Umfang der Zustimmung
  - Welcher Zweck und Rahmen?
  - Urheberrechtlicher Zweckübertragungstheorie, strenger Maßstab
- Widerruf nur unter bestimmten Voraussetzungen möglich
  - Unentgeltlich: nur bei geänderter Sachlage (4 Ob 306/70 – *Zigeunerprimas*)
  - Entgeltlich: Widerruf scheidet grundsätzlich aus, Ausnahme höchstpersönlicher Intimbereich (4 Ob 211/03p – *U-Bahn-Express*)

3. Rechtsgrundlagen – Datenschutzrecht

Einwilligung

- Strenge Anforderungen nach Art 7 DSGVO
- freiwillig
  - keine Nachteile bei Verweigerung, nicht in AGB/Verträgen versteckt, keine vorangeklickte Checkbox
- für einen bestimmten Zweck
  - nicht zu weit/generisch
- nachweisbar
- in informierter Weise
  - WER verwendet WELCHE Daten zu WELCHEM Zweck?
- jederzeit widerrufbar

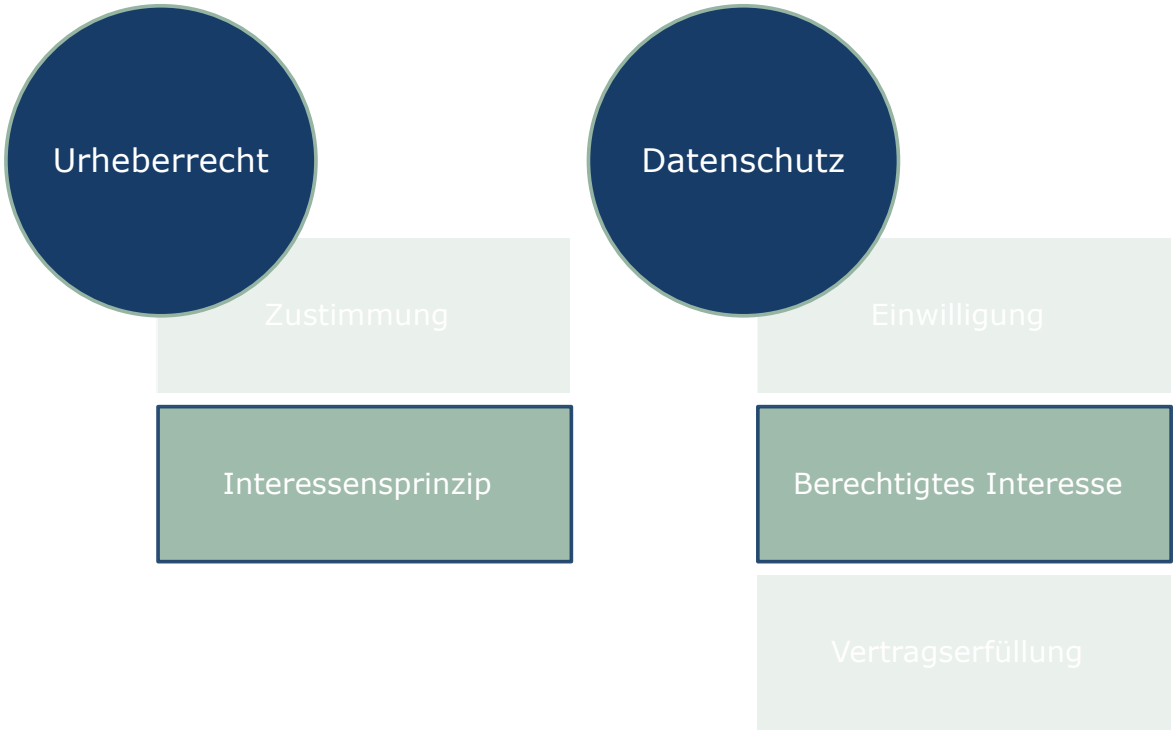
WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

3. Rechtsgrundlagen

Zustimmung vs Einwilligung

Zustimmung nach § 78 UrhG	Einwilligung nach Art 7 DSGVO
formlos	formlos, aber **nachweisbar**
auch schlüssig	**freiwillig** (nicht versteckt, aktive Handlung)
konkreter Zweck	in **informierter** Weise (inkl detaillierter Zweckbeschreibung)
Widerruf unter bestimmten Voraussetzungen	**Widerruf** jederzeit und ohne Grund möglich

3. Rechtsgrundlagen



3. Rechtsgrundlagen – Urheberrecht

Interessensprinzip

- Kein bedingungsloser Schutz gegen eine Veröffentlichung ohne Zustimmung
- Jeweils Abwägung mit Veröffentlichungsinteresse
  - Beitrag zu einer Diskussion in einer demokratischen Gesellschaft (EGMR 59320/00 – *Caroline von Hannover / Deutschland*)
- Nicht gesetzlich determiniert, *"auslegungsbedürftiger Wertungsmaßstab*"
- Erkennbarkeit als Voraussetzung für Verletzung
- Möglichkeit von Missdeutungen reicht aus
  - objektiver Maßstab, nicht subjektives Empfinden
- Sachliche Lösung unter Würdigung des Gesamtzusammenhangs

3. Rechtsgrundlagen – Urheberrecht

Interessensprinzip – Fallgruppen

- Entstellende bzw bloßstellende Bildnisse
  - Peinliche Situation, Nacktaufnahmen ("*geradezu klassischer Fall*", 4 Ob 2249/96f – *Nacktfoto(montage)*
- Verletzung der Intimsphäre
  - Aussetzen der Neugierde und Sensationslust, Krankheit (4 Ob 261/14g – *Kinderkrebsforschung*)
- Verwendung für Werbezwecke
  - Verdacht der entgeltlichen Zurverfügungstellung für Werbezwecke, betrifft auch nicht anstößige Inhalte (4 Ob 16/90 – *Thomas Muster*)
- Abträglicher Begleittext
  - Gesamtzusammenhang, nicht nur der unmittelbar beigegebene Text (4 Ob 165/08f – *Pinkelprinz*)

3. Rechtsgrundlagen – Datenschutzrecht

Berechtigtes Interesse

- Nur rudimentäre Vorgaben in der DSGVO, zu berücksichtigen:
  - rechtliche, wirtschaftliche und ideelle Interessen
  - Grundrechte und Grundfreiheiten
    - Grundrecht auf Datenschutz, Achtung des Privat- und Familienlebens, Meinungs- und Informationsfreiheit etc
  - vernünftige Erwartungen der betroffenen Person
  - Beziehung des Betroffenen zum Verantwortlichen
- Häufige Gewichtungsfaktoren in der Praxis
  - Art der Daten und Umfang der Verarbeitung
  - Potentielle Folgen der Verarbeitung für den Betroffenen (Risiko)
  - Erwartungshaltung der Betroffenen (Vorhersehbarkeit)
  - Art und Weise der Datenerhebung (heimlich vs transparent)
  - Daten zu schutzwürdigen Betroffenen (zB Kinder, Senioren oder Arbeitnehmer)

3. Rechtsgrundlagen – Datenschutzrecht

Berechtigtes Interesse

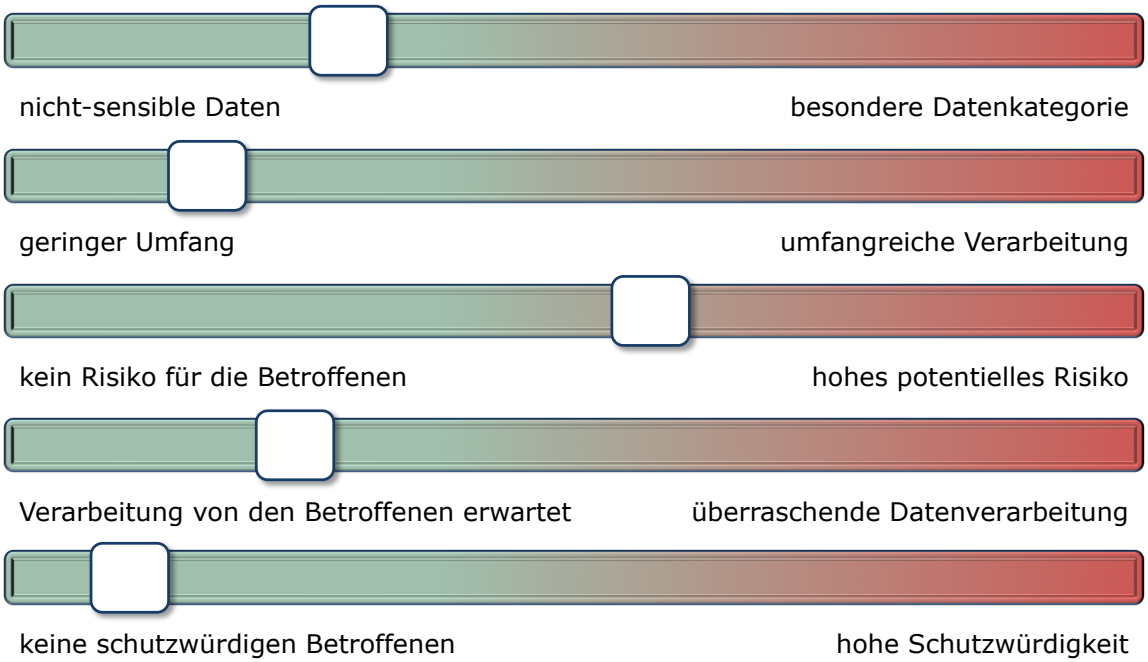
- Gesetzliche Determinierung der Interessenabwägung durch § 12 Abs 4 DSGVO:
  - jedenfalls unzulässig:
    - Kontrolle von Arbeitnehmern
    - Auswertung anhand besonderer Datenkategorien
  - nur mit ausdrücklicher (!) Einwilligung zulässig:
    - höchstpersönlicher Lebensbereich
    - Automatisierter Abgleich von Bildaufnahmen und Erstellung von Persönlichkeitsprofilen

➔ **Gesamthafte Interessenabwägung** unter Berücksichtigung der Gewichtungsfaktoren der DSGVO und der Ergänzungen des DSG

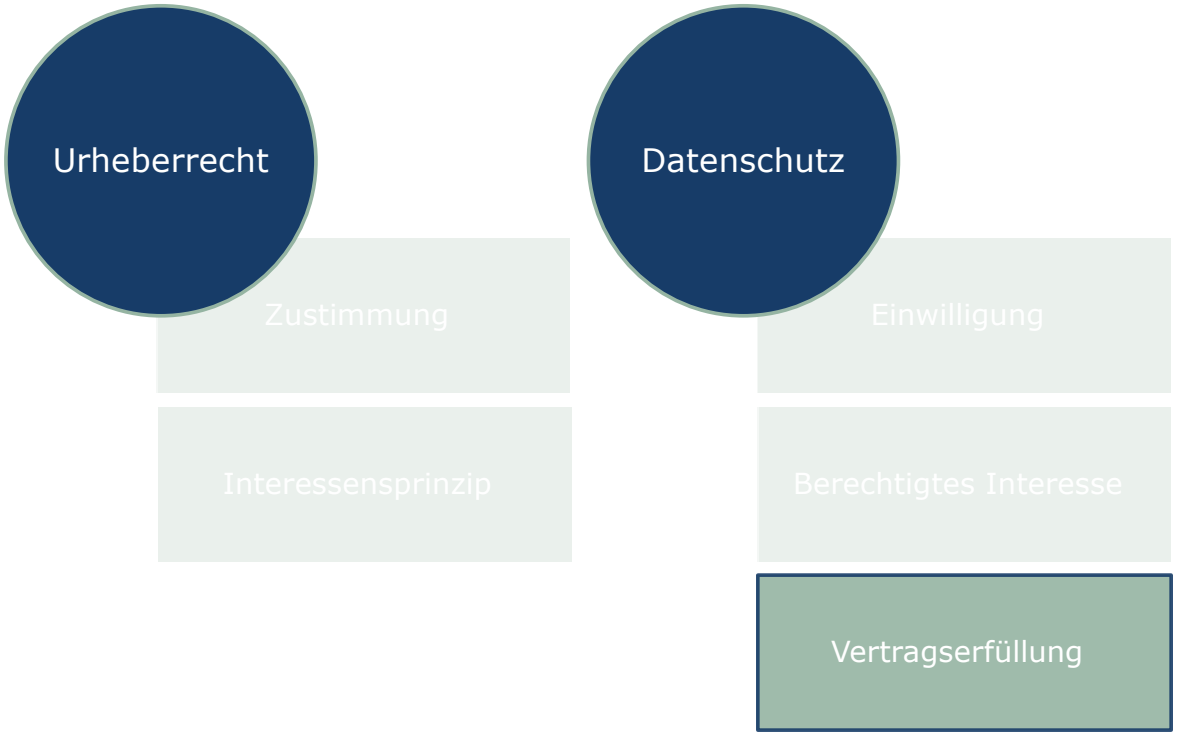
WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

3. Rechtsgrundlagen – Datenschutzrecht

Berechtigtes Interesse



3. Rechtsgrundlagen



3. Rechtsgrundlagen – Datenschutzrecht

Vertragserfüllung

- Nur bei DSGVO
  - kein eigener zivilrechtlicher Rechtfertigungsgrund
  - persönlichkeitsrechtlich: Interessenabwägung
- Verarbeitung ist zur Erfüllung eines Vertrages mit dem Abgebildeten erforderlich
  - zB Erstellung von Fotos durch vom Betroffenen beauftragten Fotografen
- nicht bei Verträgen mit Dritten
  - zB Veranstaltungsfotografie
- zweckgebunden → keine über die reine Vertragserfüllung hinausgehende Verarbeitung

4. Informationspflichten

Urheberrecht

- Keine gesetzlichen Informationspflichten
- Jedoch Berücksichtigung im Gesamtzusammenhang
- Teilweise best practice (zB bei Veranstaltungen)

DSGVO

- Betroffene müssen
- im (oder vor dem) Zeitpunkt der Aufnahme der Fotos
- umfangreich nach Art 13 bzw 14 DSGVO informiert werden
- in präziser, transparenter, verständlicher und leicht zugänglicher Form
- in klarer und einfacher Sprache
- Unabhängig von der Rechtgrundlage für die Aufnahme!

4. Informationspflichten

DSGVO

- Mindestinhalt der Information an Betroffene:
  - datenschutzrechtlicher Verantwortlicher
  - Zwecke der Aufnahmen bzw Fotonutzung
  - Rechtsgrundlage
  - gegebenenfalls Empfänger der Aufnahmen
  - Speicherdauer
  - Rechte des Betroffenen

➔ DSGVO hat Informationspflichten wesentlich **erweitert**

- Umsetzung in der Praxis:
  - Datenschutzhinweise und/oder
  - Aushang

5. Ausgewählte Praxisfälle

Veranstaltungsfotografie

Berechtigte Interessen argumentierbar, sofern

- öffentliche Veranstaltung
- großflächige Aufnahmen
- größerer Personenkreis
- gewöhnliche, nicht bloßstellende Situationen

sonst Einwilligung/Zustimmung

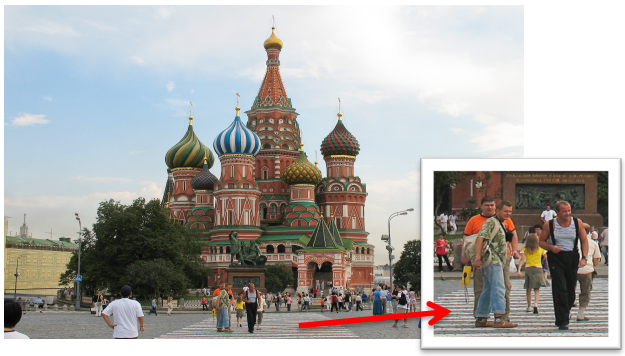
- zB Weihnachtsfeiern oder interne Sportveranstaltungen

Umsetzung in der Praxis

- deutlicher Hinweis auf Fotoaufnahmen (Aushang, Datenschutzerklärung)
- keine bloßstellende Situationen einfangen/veröffentlichen
- Erwartungshaltung der Besucher berücksichtigen (insb auch hinsichtlich Umfang und Medium bei der Veröffentlichung)

5. Ausgewählte Praxisfälle

Öffentliche Flächen



grds **berechtigtes Interesse**

- Passanten, müssen idR Einbeziehung hinnehmen, wenn sie öffentlichen Raum benützen.

Einwilligung/Zustimmung, sofern

- Alltagssituation verlassen (nicht nur beiläufig aufgenommene Personen)

Gruppengröße: keine "Daumenregel", aber Kriterium bei Abwägung

5. Ausgewählte Praxisfälle

Werbezwecke

5. Ausgewählte Praxisfälle

Werbezwecke

<table>
<tr><th>Entgeltliche Aufnahmen</th><th>Unentgeltliche Aufnahmen</th></tr>
<tr><th colspan="2">UrhG</th></tr>
<tr><td colspan="2">zumindest schlüssige Zustimmung erforderlich</td></tr>
<tr><td colspan="2">Vertragstext bzw Erwartungshaltung des Betroffenen grenzen zulässigen Nutzungsumfang ab: im Zweifel nur konkretes Projekt</td></tr>
<tr><td>Zustimmung grds nicht widerrufbar (außer höchstpersönlicher Intimbereich)</td><td>Zustimmung nur bei geänderter Sachlage widerrufbar</td></tr>
<tr><th colspan="2">DSGVO</th></tr>
<tr><td rowspan="2">Datenverarbeitung zur Vertragserfüllung erforderlich (sofern Beweggründe und Zielsetzung der Nutzung der Aufnahmen für den Betroffenen klar vorhersehbar)</td><td>Berechtigtes Interesse oder Einwilligung</td></tr>
<tr><td>etwaige Einwilligung jederzeit ohne Grund widerrufbar</td></tr>
</table>

6. Wesentliche Rechte der Abgebildeten

Widerruf – Widerspruch – Löschung

- **Widerruf** der Einwilligung
- **Widerspruch** bei Verarbeitung auf Basis berechtigter Interessen
  - neue Interessensabwägung aufgrund "*besonderer Situation*"
  - Wirkung für die Zukunft
- **Löschung** (in allen Systemen!) sofern ein Löschungsgrund vorliegt
  - zB Datenverarbeitung nicht mehr notwendig oder sonst unrechtmäßig, berechtigter Widerruf oder Widerspruch

1. Daten "*unverzüglich*" löschen (Art 17 Abs 1)
2. bei Veröffentlichung: "*angemessene Maßnahmen*" treffen, um andere Verantwortliche über Löschung aller Links, Kopien oder Replikationen zu informieren (Art 17 Abs 2)
3. bei Offenlegung an Dritte: Empfänger über die Löschung informieren, sofern nicht "*unmöglich*" oder "*unverhältnismäßiger Aufwand*" (Art 19)

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

6. Wesentliche Rechte der Abgebildeten

UrhG

- Urheber-/Persönlichkeitsrechtlicher Anspruchskatalog
  - **Unterlassung** (§ 81 UrhG)
  - **Beseitigung** (§ 82 UrhG)
    - Vernichtung der Eingriffsgegenstände, Unbrauchbarmachung der Eingriffsmittel
    - Jedoch Vorbehalt der Verhältnismäßigkeit (Art 10 Abs 3 DurchsetzungsRL: keine zwecklose Wertvernichtung)
    - Möglichkeiten der Schwärzung, Entfernung einzelner Seiten
    - Richtet sich nach Art und Gegenstand des Einzelfalls (4 Ob 274/02a)
    - Rückrufanspruch: in Ausnahmefällen, Voraussetzung Verfügungsgewalt

    ➔Wertungsübernahme für DSGVO?
  - **Urteilsveröffentlichung** (§ 85 UrhG)
  - **Schadenersatz** (§ 87 UrhG)

7. Fazit

- Keine komplette Abkehr von bestehenden Grundsätzen
- Viele DSGVO-Aspekte bereits im zivilrechtlichen Bildnisschutz vorgezeichnet
- Übernahme von Wertungen möglich
- Rechtsfolgen und Ansprüche nach DSGVO und UrhG bestehen nebeneinander
- Wesentlichste Neuerungen durch die DSGVO
  - Strengere Anforderungen an die Einwilligung
  - Stärkere Bedeutung der korrekten Rechtsgrundlage (jederzeitige Widerrufbarkeit der Einwilligung)
  - Ausgedehnte Informationspflichten
  - Gestärkte Rechte der Betroffenen

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Ansprechpartner

Dr Andreas Seling, M.B.L.

- seit 2010 bei DORDA
- Seit 2014 Rechtsanwalt im IT/IP und Media Team
- Universität Salzburg, Mag iur 2006, Dr iur 2010
- Fachliche Schwerpunkte:
  - Lauterkeitsrecht
  - Marken- und Musterrecht
  - Urheber- und Medienrecht
  - Social Media
  - E-Commerce
- Autor zahlreicher Fachpublikationen
- Vortragender an diversen Hochschulen, bei Fachtagungen und Veranstaltungen

Ansprechpartner

Mag Dominik Schelling

- seit 2011 bei DORDA
- Rechtsanwaltsanwärter im IP/IT/Datenschutz Team
- Universität Wien, Mag iur 2014
- Rechtsanwaltsprüfung 2018
- Fachliche Schwerpunkte:
  - IT-Recht
  - Datenschutzrecht
  - Urheber-, Wettbewerbs- und Medienrecht
  - Immaterialgüterrecht
  - E-Commerce
  - Outsourcing-Projekte
  - Blockchain
- Datenschutzbeauftragter diverser Unternehmen in verschiedensten Branchen
- Autor von Fachpublikationen in den Bereichen IP/IT, Datenschutz und E-Commerce
- Regelmäßig Vortragender bei Fachseminaren

WIR SCHAFFEN KLARHEIT. INFOLAW WWW.INFOLAW.AT DORDA

Dr Andreas Seling, M.B.L.
T: +43 1 533 47 95 - 23
E: andreas.seling@dorda.at

Mag Dominik Schelling
T: +43 1 533 4795-23
E: dominik.schelling@dorda.at

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien

International Law Office - Information Technology Award for Austria 2014, 2015, 2016, 2017, 2018 & 2019
International Law Office - E-Commerce Award for Austria 2012 & 2013
JUVE - Austrian Law Firm of the Year 2017

KNYRIM.TRIEB RECHTSANWÄLTE

KNYRIM.TRIEB RECHTSANWÄLTE

13. IT-Rechtstag

1 Jahr DSGVO –
Erste Erfahrungen und Problembereiche

Dr. Rainer Knyrim
Rechtsanwalt und Partner
Knyrim Trieb Rechtsanwälte, Wien

KNYRIM.TRIEB
RECHTSANWÄLTE


TeachPrivacy
www.teachprivacy.com
I can fly.
I can throw a car.
I can scare criminals.
I can make executives pay attention to privacy.
GDPR
We're so not worthy!
Written by Daniel J. Solove
Illustrated by Ryan Beckwith
For personal use only. Please ask us for permission for other uses.


This year, the security budget will be $10 million.
What? That's all?
This year, the privacy budget will be $100,000.
Wow! Thanks for the big increase!
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith

KNYRIM.TRIEB
RECHTSANWÄLTE

Umsetzung der DSGVO in der Unternehmenspraxis

KNYRIM.TRIEB RECHTSANWÄLTE

I. Google

KNYRIM.TRIEB RECHTSANWÄLTE

CNIL - Google

Französische Datenschutzbehörde CNIL verhängt am 21.1.2019 gegen Google **EUR 50 Mio Strafe.**

Warum?

KNYRIM.TRIEB RECHTSANWÄLTE

CNIL - Google

Grund der Strafe:

1. **Verstoß gegen Informationspflichten:**

- **Angaben zum Teil über mehrere Dokumente verstreut** und erst mit 5-6 Arbeitsschritten (Klicks) abrufbar gewesen.
- Nicht ausreichend konkrete **Angaben zu Löschfristen**
- Es fehlte: „**präzise, transparente, verständliche und leicht zugängliche Form** in einer klaren und einfachen Sprache“ – siehe Art 12 Abs 1 DSGVO

KNYRIM.TRIEB RECHTSANWÄLTE

CNIL - Google

Grund der Strafe:

2. Unzureichende Einwilligungen für personalisierte Werbung:

- Einwilligung **entsprach nicht den Vorgaben der DSGVO** – freiwillig, informiert, Bezug auf bestimmten Fall, unmissverständliche Willensbekundung
- Insbes. **Verstoß gg. ErwGr 43**: Einwilligung nicht freiwillig erteilt, wenn **zu verschiedenen Verarbeitungsvorgängen nicht gesonderte Einwilligung erteilt werden kann**, obwohl dies im Einzelfall angebracht ist.“

KNYRIM.TRIEB RECHTSANWÄLTE

CNIL - Google

Konsequenz für Unternehmen:

- **Kritikpunkte der Entscheidung lesen und verstehen; Leitlinien der Art. 29-Gruppe** WP 259 und 260 **zu Transparenz und Einwilligung lesen**
- **Eigene Datenschutzinformation danach gestalten!**
- **„Noch deutlich schwieriger – oder aufwändiger – dürfte es für viele Unternehmen werden, die hohen Anforderungen der CNIL in Bezug auf das Einholen von auf den jeweiligen Einzelfall zugeschnittenen Einwilligungen umzusetzen.“ (Wybitul, ZD 3/2019, 98).**

KNYRIM.TRIEB RECHTSANWÄLTE

II. Allergie-Tagesklinik

DSB 16.11.2018, DSB-D213.692/0001-DSB/2018, veröffentlicht März 2019

KNYRIM.TRIEB RECHTSANWÄLTE

DSB - Allergie-Tagesklinik

Befunde per Mail? Keine Frage der Einwilligung

Datenschutz. Behörde verlangt von Ärzten und Unternehmen wesentlich größere Sorgfalt.

VON RAINER KNYRIM

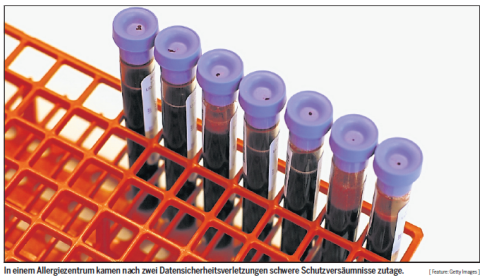
Wien. Im Stress rund um die Einführung der Datenschutz-Grundverordnung haben viele Unternehmen versucht, in kürzester Zeit die datenschutzrechtlichen Anforderungen „irgendwie" hinzubekommen. Ohne sich eingehender mit der Materie auseinanderzusetzen, wurden Informationstexte für die eigenen Homepages und Einwilligungen für Kunden nach zirkulierenden Texten erstellt, Informationen und Muster der eigenen Kammern unreflektiert übernommen und vermeintliche „Patentlösungen" eingeführt. Die Braut wurde für den 25. Mai herausgeputzt, oftmals ohne dass viel dahinter stand.

Was dabei herauskommt, zeigt ein Bescheid der Datenschutzbehörde, der vorige Woche im Rechtsinformationssystem veröffentlicht wurde: Der Datenschutz-Koordinator eines Allergie-Tageszentrums meldete bei der Behörde zweimal (verpflichtend) Sicherheitsverletzungen ein; der Behörde fiel offensichtlich auf, dass laut der Datenschutzinformation auf der Homepage des Allergiezentrums aber ein Datenschutzbeauftragter bestellt war, den es gar nicht gab. Die Datenschutzinformationen auf der Webseite an, ebenso die Einwilligungserklärung der Patienten. Sie stellte einige Fragen, ließ sich das Verarbeitungsverzeichnis schicken und konnte dadurch zahlreiche Unverträglichkeiten mit dem Datenschutzrecht feststellen. Das Ergebnis war ein Bescheid, der nicht weniger als vierzehn einzelnen Mängel auflistet (siehe unten).

Der Inhalt betrifft zunächst sämtliche Ärzte und Ärztegemeinschaften: Die Datenschutzbehörde erklärte die mittlerweile sehr verbreitete Methode für gesetzwidrig: Statt ihre technischen Sicherheitsmaßnahmen bei der Datenübermittlung zu erhöhen und E-Mails zu verschlüsseln, lassen Ärzte die Patienten eine Einwilligungserklärung unterschreiben, dass sie einer unverschlüsselten Übermittlung ihrer Befunde zustimmen. Die Frage, ob eine Übermittlung von ratungsfunktion und muss in bestimmten Fällen verpflichtend bestellt werden, etwa dann, wenn die Kerntätigkeit des Unternehmens in der umfangreiche Verarbeitung von Gesundheitsdaten besteht.

Langes Sündenregister

Die Datenschutzbehörde sah sich



In einem Allergiezentrum kamen nach zwei Datensicherheitsverletzungen schwere Schutzversäumnisse zutage. [Feature: Getty Images]

Mitarbeiter – eine deutliche Warnung, dass es sich im Detail mit den verschiedenen Pflichten des Datenschutzrechts befassen muss. All jene, die gehofft hatten, dass Oberflächlichkeit reicht und die Datenschutzbehörde sie im Ernstfall schon beraten werde, enttäuscht die Datenschutzbehörde: Auf deren Frage warum das Allergiezentrum keinen Datenschutzbeauftragten bestellt habe, antwortet dieses mit der Feststellung, dass man eine vor dem 25. Mai 2018 erfolgte Information der Ärztekammer und der WKO so verstanden habe, dass man keinen brauche, sich aufgrund einer neuen Information aber nun nicht mehr sicher sei und die Behörde um eine „Empfehlung" bitte.

Datenschutzbeauftragter fehlt

Die Behörde „empfiehlt" in dem

linien der europäischen Datenschutzbehörden zu dieser Frage selbst hätte zum Schluss kommen müssen, dass ein Datenschutzbeauftragter zu bestellen gewesen sei. Selbiges macht die Datenschutzbehörde bei der Feststellung, dass die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gleich bei sechs (!) Datenanwendungen, die das Unternehmen betreibt, verletzt wurde, und die Pflicht auch aus der DSGVO „klar hervorgehe"; die Behörde verwies wieder auf die Leitlinien der europäischen Datenschutzbehörden.

Der Bescheid ist angesichts der Mannigfaltigkeit der Rechtsverstöße, die die Behörde bei einem kleinen Unternehmen feststellte und der Direktheit, mit der die Nichtbefassung mit Datenschutzrecht vorgeworfen wird, geradezu spektakulär. Ob im Anschluss an das Prüfverfahren ein Verwaltungsstrafverfahren zur Verhängung einer Geldstrafe eingeleitet wurde, geht aus dem vorliegenden Bescheid nicht hervor. Das Unternehmen wird mit der Umsetzung der aufgetragenen Pflichten binnen der gesetzten acht Wochen aber ohnehin schon erheblichen Aufwand haben. Datenschutz-Allergiker seien vor der Lektüre der unten stehenden Zusammenfassung des Bescheidspruchs gewarnt: Nebenwirkungen sind nicht auszuschließen, eine Therapie wird dringend empfohlen.

Dr. Rainer Knyrim ist Gründungspartner von Knyrim Trieb Rechtsanwälte.

KNYRIM.TRIEB RECHTSANWÄLTE

DSB - Allergie-Tagesklinik – Einwilligung

Aus der Datenschutzinformation des Unternehmens:

Für welche Zwecke und auf welcher Rechtsgrundlage werden die Daten verarbeitet?

*Die Allergie-Tagesklinik D*** verarbeitet Ihre personenbezogenen Daten im Einklang mit den Bestimmungen der DSGVO und dem Datenschutz-Anpassungsgesetz 2018:*

- *zur Erfüllung von vertraglichen Pflichten (Art 5 Abs 1b DSGVO)*

Dokumentationspflicht gem. & 51 Ärztegesetz sowie die Erfassung sämtlicher Leistungen einschließlich automationsunterstützt erstellter und archivierter Textdokumente in diesen Angelegenheiten, etc.

- *zur Erfüllung rechtlicher Verpflichtungen (Art 6 Abs 1c DSGVO)*

Eine Verarbeitung personenbezogener Daten kann zum Zweck der Erfüllung unterschiedlicher gesetzlicher Verpflichtungen (Ärztegesetz, etc.) oder aus steuer- sowie unternehmensrechtlichen Vorgaben erforderlich sein.

- *im Rahmen Ihrer Einwilligung (Art 6 Abs 1a DSGVO)*

*Wenn Sie der Allergie-Tagesklinik D*** eine Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten erteilt haben, erfolgt eine Verarbeitung zu gemäß den in der Zustimmungserklärung festgelegten Zwecken und im darin vereinbarten Umfang. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.*

- *zur Wahrung berechtigter Interessen (Art 6 Abs 1f DSGVO).*

KNYRIM.TRIEB RECHTSANWÄLTE

DSB - Allergie-Tagesklinik – Einwilligung

DSB dazu:

„Zunächst ist der **Einwilligung nicht mit der erforderlichen Klarheit zu entnehmen, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage darstellt.** In der bereitgestellten Information nach Art. 13 DSGVO wird als Rechtsgrundlage zwar die **Einwilligung genannt, es werden jedoch auch andere Rechtsgrundlagen, wie bspw. die Erfüllung rechtlicher Verpflichtungen oder die Wahrung berechtigter Interessen angeführt**. Insofern ist unklar, für welche konkreten Datenverarbeitungen die Einwilligung die Rechtsgrundlage ist.“

KNYRIM.TRIEB RECHTSANWÄLTE

DSB - Allergie-Tagesklinik – Einwilligung

× Ich bin ausdrücklich damit einverstanden, dass personenbezogene Daten (insb. Informationen über meinen Zustand bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf, meine Befunde sowie Informationen über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten) verarbeitet, gespeichert und in unverschlüsselter Form an die und von den dementsprechend relevanten Dritten geschickt werden. Die Zustimmung über den unverschlüsselten Versand kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Ich stimme weiters unwiderruflich zu, dass die Allergie-Tagesklinik D*** jederzeit andere Unternehmen und/oder Personen zur Durchführung der vereinbarten Dienstleistung heranziehen darf. Dies betrifft auch die Verarbeitung inkl. Speicherung von personenbezogenen Daten. Ich nehme zur Kenntnis, dass durch die Übermittlung der Daten (unberechtigte) Dritte Kenntnis über die Informationen erhalten können und diese Daten verändert werden können. Mir ist bewusst, dass dies zur Offenlegung meines Gesundheitszustandes führen kann. Mir ist bewusst, dass die Allergie-Tagesklinik D*** keinerlei Haftung für die korrekte und vollständige Übermittlung der Daten übernehmen kann.

KNYRIM.TRIEB RECHTSANWÄLTE

DSB – Allergie-Tagesklinik Einwilligung

- **DSB: Unzulässige Einwilligung**
- Erklärung erfasst Tatbestände, die **keiner Einwilligung** unterliegen, jedoch den **Anschein erwecken**, dass hierfür eine Einwilligung zu erteilen ist
  - **Frage, ob eine Übermittlung in verschlüsselter oder unverschlüsselter Form erfolgt, ist eine Datensicherheitsmaßnahme nach Art 32 DSGVO und somit vom Verantwortlichen alleine zu beurteilen und keiner Einwilligung zugänglich**
  - **Die Heranziehung von Auftragsverarbeitern** ist einer Einwilligung von Betroffenen nicht zugänglich
  - Eine „**unwiderrufliche**“ Einwilligung widerspricht jedenfalls Art 7 Abs 3 DSGVO

KNYRIM.TRIEB RECHTSANWÄLTE

Beispiel eines Allergiezentrums, Stand 19.3.2019

☐ **Einwilligungserklärung zur E-Mail-Übermittlung für Patienten:**

Ich stimme ausdrücklich zu, dass das Allergiezentrum Wien West Informationen aus meiner Patientendokumentation (insb. Befunde, Rezepte, Überweisungen, Stammdaten, Informationen über Zustand bei Übernahme der Beratung oder Behandlung, Vorgeschichte einer Erkrankung, Diagnose, Krankheitsverlauf sowie Informationen über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Medikation) in unverschlüsselter Form an die von mir bekanntgegebene E-Mail-Adresse übermitteln darf. Die Rechtmäßigkeit der Verarbeitung meiner Daten bleibt bis zum Einlangen des Widerrufs davon unberührt.

Wien, am ..... X .....

Unterschrift Patient/Patientin

- bei Personen ab 18 Jahren unterschreibt der Erwachsene
- Kinder ab 14 Jahre: Unterschrift eines/einer Erziehungsberechtigten plus Unterschrift Kind
- Kinder unter 14 Jahre: Unterschrift eines/r Erziehungsberechtigten

Unterschreibt ein Elternteil als Erziehungsberechtigte/r allein, so erklärt sie/er mit ihrer/seiner Unterschrift, dass ihr/ihm das Sorgerecht allein zusteht oder dass sie/er im Einverständnis mit dem anderen Elternteil handelt.

Datenschutz, Stand 12.03.2019 1/1 Vorbehaltlich Satz-, Druck- und Rechenfehler

KNYRIM.TRIEB RECHTSANWÄLTE

Muster Ärztekammer Wien, Stand 16.3.2019

Muster für eine Einwilligungserklärung

Einwilligungserklärung E-Mailübermittlung für Patienten

"Ich stimme zu, dass bis auf Widerruf mein/e behandelnde/r Ärztin/Arzt sämtliche Informationen aus meiner Patientendokumentation (somit Informationen über meinen Zustand bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten) an die folgende E-Mailadresse mittels unverschlüsselter E-Mail senden darf:

_____

Ich nehme zur Kenntnis, dass durch die Übermittlung der Daten (unberechtigte) Dritte Kenntnis über die Informationen erhalten können und diese Daten verändert werden können. Mir ist bewusst, dass dies zur Offenlegung meines Gesundheitszustandes führen kann.

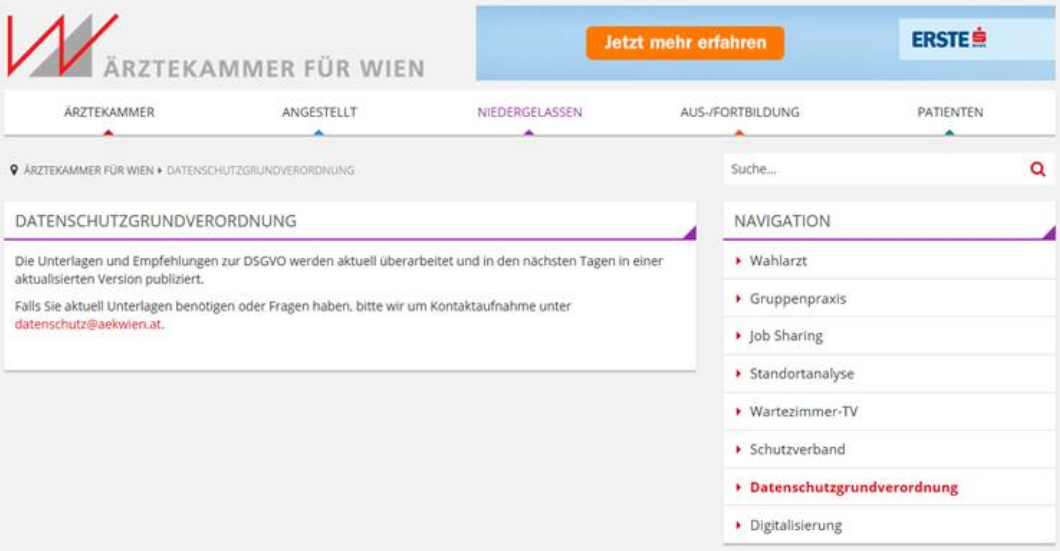
Diese Einwilligung kann jederzeit widerrufen werden. Die Rechtmäßigkeit der Verarbeitung meiner Daten bleibt bis zum Einlangen des Widerrufs davon unberührt.

_____

Datum Unterschrift

KNYRIM.TRIEB RECHTSANWÄLTE

Muster Ärztekammer Wien, Stand 14.5.2019



KNYRIM.TRIEB RECHTSANWÄLTE

DSB – Allergie-Tagesklinik – DSFA

- **Verstoß** gegen die **Pflicht zur Prüfung der Notwendigkeit einer Datenschutz-Folgenabschätzung**
- **Ausnahmetatbestand DSFA-A12** (Patientenverwaltung) der Anlage zur **DSFA-AV** ist nach den Erläuternden Bemerkungen der DSB nur erfüllt, wenn sie von einem **einzelnen Arzt** geführt wird
- **DSFA-AV** und **DSFA-V** enthalten **keine abschließenden Aufzählungen**, sondern nur Verarbeitungsvorgänge, die jedenfalls einer oder keiner DSFA unterliegen
- Ist ein Verarbeitungsvorgang **nicht** durch eine der beiden **Verordnungen gedeckt**, muss der **Verantwortliche im Einzelfall prüfen, ob eine DSFA erforderlich ist oder nicht**
- Als Hilfestellung können die **Leitlinien der Art 29-Datenschutzgruppe** zur DSFA herangezogen werden (WP 248 rev.01)

KNYRIM.TRIEB RECHTSANWÄLTE

DSB – Allergie-Tagesklinik – DSFA

Dazu ist auszuführen, dass die Verantwortliche schon aus den erläuternden Bemerkungen (abrufbar auf der Website der Datenschutzbehörde) hätte feststellen müssen, dass die Patientenverwaltung – begrenzt auf den Gegenstand der Verwaltung der Datensätze, die üblicher Weise auch bei einer Kundenverwaltung anfallen – nur dann nicht einer DSFA zu unterziehen ist, wenn sie von einem einzelnen Arzt geführt wird.

Für die Verarbeitungstätigkeiten

- Patientenakten (Adress-, Rechnungs- und Meldedaten)
- Abrechnung (Abrechnung mit der Sozialversicherung)
- Befundanforderung/Befundübermittlung (Übermittlung und Offenlegung),
- Untersuchung von Proben (Untersuchung und Versand von Proben [Blut

KNYRIM.TRIEB RECHTSANWÄLTE

DSB – Allergie-Tagesklinik – Zusammenfassung

14 Verstöße bei einem Unternehmen

Bescheid. Datenschutzbehörde räumt acht Wochen Umsetzungsfrist ein.

Wien. Die Datenschutzbehörde hat im amtswegigen Prüfverfahren gegen ein Unternehmen, eine Allergie-Tagesklinik, 14 Pflichtverletzungen festgestellt. Die Datenschutz-Grundverordnung wurde in folgenden Punkten verletzt (DSB-D213.692/0001-DSB/2018):

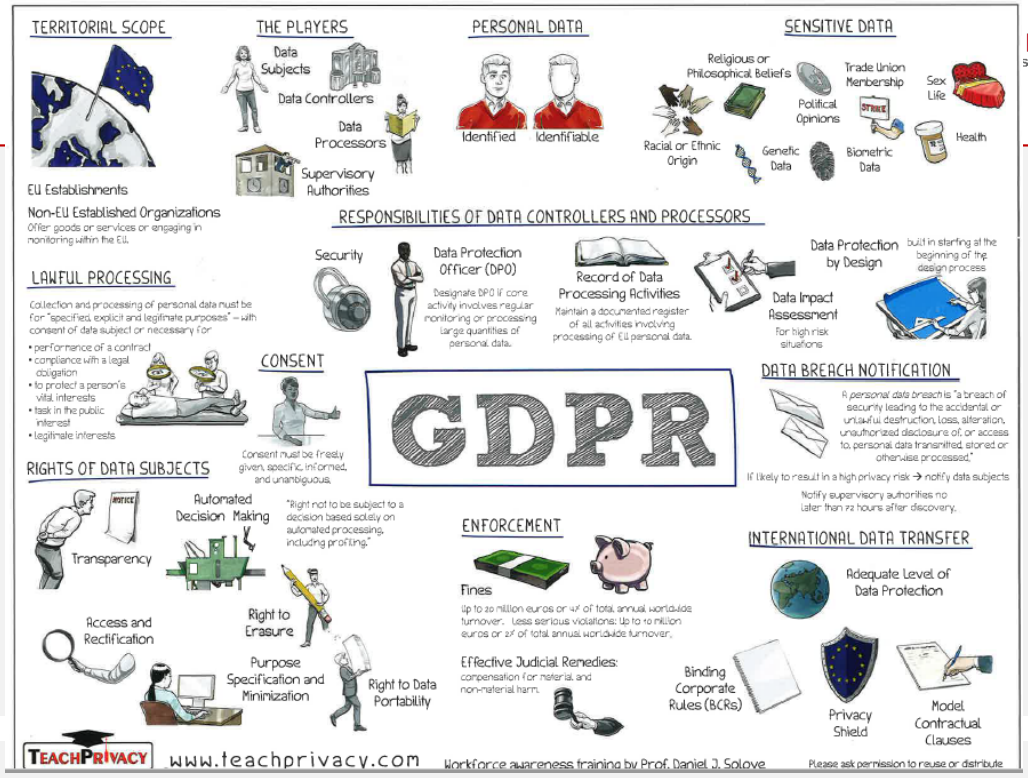
Einwilligung. Das Unternehmen hat Betroffene mit seiner Einwilligungserklärung zu einer gesetzwidrigen Einwilligung verpflichtet. Denn a) erfasst die Erklärung Tatbestände, die keiner Einwilligung unterliegen, jedoch den Anschein erwecken, dass hierfür eine Einwilligung zu erteilen ist, und b) war ihr nicht mit hinreichender Klarheit zu entnehmen, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage ist.

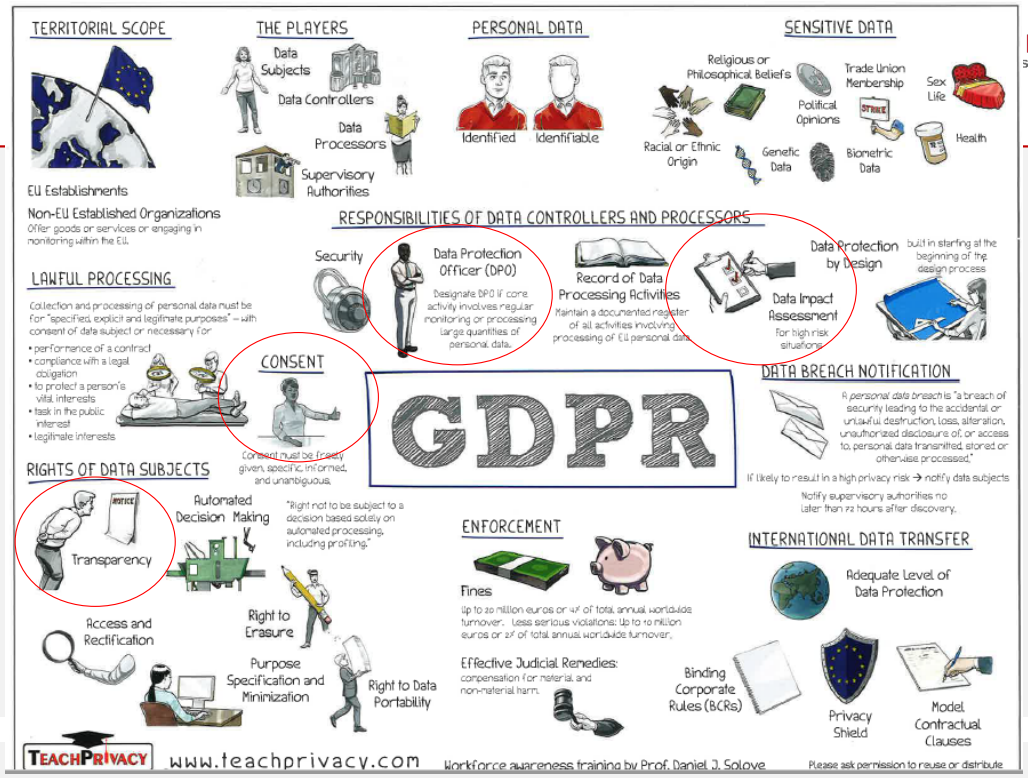
Informationspflichten. Das Unternehmen hat gegen die Informationspflichten verstoßen, da es im „Informationsblatt zum Datenschutz" bzw. online a) nicht deutlich unterschieden hat, ob die Informationen nach Art 13 oder nach Art 14 DSGVO erteilt werden, b) den Namen und die Kontaktdaten eines nicht bestellten Datenschutzbeauftragten angegeben hat, c) die Rechtsgrundlagen für die Verarbeitung unvollständig angeführt hat, d) nicht angeführt hat, worin die berechtigten Interessen, die von der Verantwortlichen verfolgt werden, bestehen, e) nicht angeführt hat, dass die Einwilligung jederzeit widerrufen werden kann, ohne dass dadurch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.

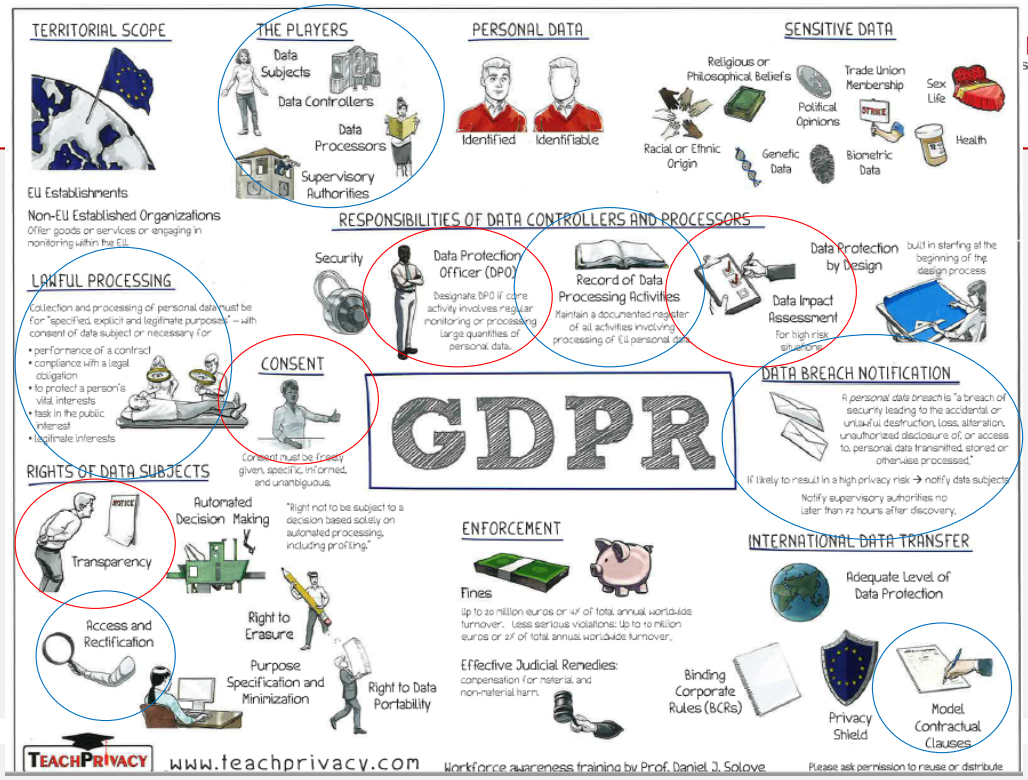
Datenschutz-Folgenabschätzung. Das Unternehmen hat gegen die Pflicht zur Prüfung der Notwendigkeit einer Durchführung von Datenschutz-Folgenabschätzungen betreffend folgende sechs Verarbeitungstätigkeiten verstoßen, indem es in unzutreffender Weise davon ausging, dass jedenfalls keine Datenschutz-Folgenabschätzungen durchzuführen sind: a) Patientenakten (Adress-, Rechnungs- und Meldedaten), b) Abrechnung (Abrechnung mit der Sozialversicherung), c) Befundanforderung/Befundübermittlung (Übermittlung und Offenlegung), d) Untersuchung von Proben (Untersuchung und Versand von Proben, Blut, Sekret etc.), e) Verwaltung von Rezepten (Speicherung, welche Rezepte Patienten benötigen), f) Hausapotheke (Betrieb, Verwaltung, Abrechnung und Organisation der Hausapotheke),

Datenschutzbeauftragter. Das Unternehmen hat gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten verstoßen.

Konsequenz. Als Konsequenz trug die Datenschutzbehörde dem Unternehmen auf, innerhalb einer Frist von acht Wochen bei sonstiger Exekution einen Datenschutzbeauftragten zu bestellen und der Datenschutzbehörde zu melden und ihre Einwilligungserklärung sowie ihr „Informationsblatt zum Datenschutz" bzw. die Information auf der Website rechtskonform zu gestalten und zu prüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist und eine diesbezügliche Meldung an die Behörde zu erstatten.


TERRITORIAL SCOPE
EU Establishments
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.
THE PLAYERS
Data Subjects
Data Controllers
Data Processors
Supervisory Authorities
PERSONAL DATA
Identified
Identifiable
SENSITIVE DATA
Religious or Philosophical Beliefs
Trade Union Membership
Sex Life
Political Opinions
Racial or Ethnic Origin
Genetic Data
Biometric Data
Health
RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS
Security
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.
Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.
Data Protection by Design
built in starting at the beginning of the design process
Data Impact Assessment
for high risk situations
LAWFUL PROCESSING
Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for
• performance of a contract
• compliance with a legal obligation
• to protect a person's vital interests
• task in the public interest
• legitimate interests
CONSENT
Consent must be freely given, specific, informed, and unambiguous.
GDPR
DATA BREACH NOTIFICATION
A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
If likely to result in a high privacy risk → notify data subjects
Notify supervisory authorities no later than 72 hours after discovery.
RIGHTS OF DATA SUBJECTS
Transparency
Automated Decision Making
"Right not to be subject to a decision based solely on automated processing, including profiling."
Right to Erasure
Access and Rectification
Purpose Specification and Minimization
Right to Data Portability
ENFORCEMENT
Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.
Effective Judicial Remedies:
compensation for material and non-material harm.
INTERNATIONAL DATA TRANSFER
Adequate Level of Data Protection
Binding Corporate Rules (BCRs)
Privacy Shield
Model Contractual Clauses
TEACHPRIVACY
www.teachprivacy.com
Workforce awareness training by Prof. Daniel J. Solove
Please ask permission to reuse or distribute


TERRITORIAL SCOPE
EU Establishments
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.
THE PLAYERS
Data Subjects
Data Controllers
Data Processors
Supervisory Authorities
PERSONAL DATA
Identified
Identifiable
SENSITIVE DATA
Religious or Philosophical Beliefs
Trade Union Membership
Sex Life
Political Opinions
Racial or Ethnic Origin
Genetic Data
Biometric Data
Health
RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS
Security
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.
Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.
Data Protection by Design
built in starting at the beginning of the design process
Data Impact Assessment
for high risk situations
LAWFUL PROCESSING
Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for
• performance of a contract
• compliance with a legal obligation
• to protect a person's vital interests
• task in the public interest
• legitimate interests
CONSENT
Consent must be freely given, specific, informed, and unambiguous.
GDPR
DATA BREACH NOTIFICATION
A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
If likely to result in a high privacy risk → notify data subjects
Notify supervisory authorities no later than 72 hours after discovery.
RIGHTS OF DATA SUBJECTS
Transparency
Automated Decision Making
"Right not to be subject to a decision based solely on automated processing, including profiling."
Right to Erasure
Access and Rectification
Purpose Specification and Minimization
Right to Data Portability
ENFORCEMENT
Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.
Effective Judicial Remedies:
compensation for material and non-material harm.
INTERNATIONAL DATA TRANSFER
Adequate Level of Data Protection
Binding Corporate Rules (BCRs)
Privacy Shield
Model Contractual Clauses
TEACHPRIVACY
www.teachprivacy.com
Workforce awareness training by Prof. Daniel J. Solove
Please ask permission to reuse or distribute



Vielen Dank für Ihre Aufmerksamkeit!

RA Dr. Rainer Knyrim

Knyrim Trieb Rechtsanwälte OG

1060 Wien, Mariahilfer Straße 89a

Tel. +43/1/9093070, Fax +43/1/9093639,

Email ky@kt.at

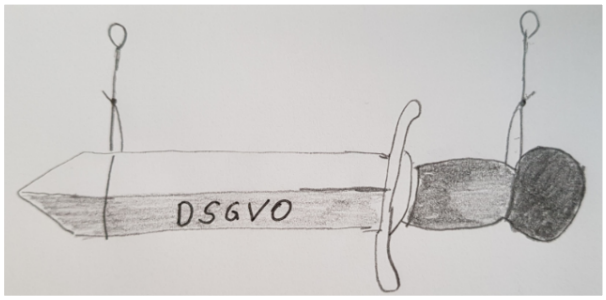
Datenschutz-Newsletter: www.kt.at

1 Jahr DSGVO

24. Mai 2019

Drei. Macht's einfach.

Vor dem 25. Mai 2018 ist danach.



GDPR als „Damoklesschwert" sorgt weiter für gewisse Unsicherheit

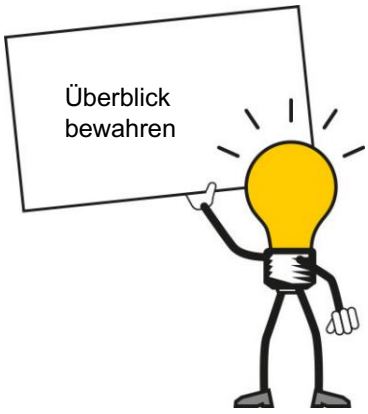
Drei muss die GDPR als permanenten Begleiter überall hin mitnehmen

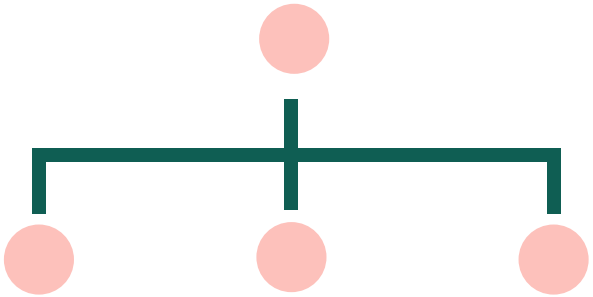
Herausforderung: DSGVO intern verständlich machen.

- Datenschutzhandbuch
- Richtlinien, Checklisten
- VVZ elektronisch mit Genehmigungsprozess
- DPIA template
- Interne Kommunikation
- Schulungen
- Datenschutzsprechstunde der DPO
- Verfahrensverzeichnis in Sharepoint, für alle einsehbar
- Etablierter Prozess für Datenschutzfolgeabschätzungen
- 4 Augenprinzip DPO/CISO

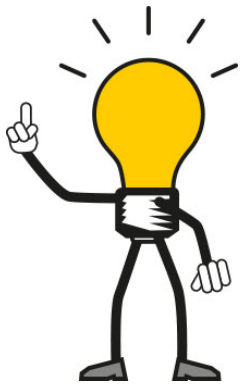
Mach´s einfach und rede darüber!

Struktur hilft





Der/die Datenschutzbeauftragte wird's schon richten. ?



Datenschutz ist Bringschuld des Datenschutzbeauftragten

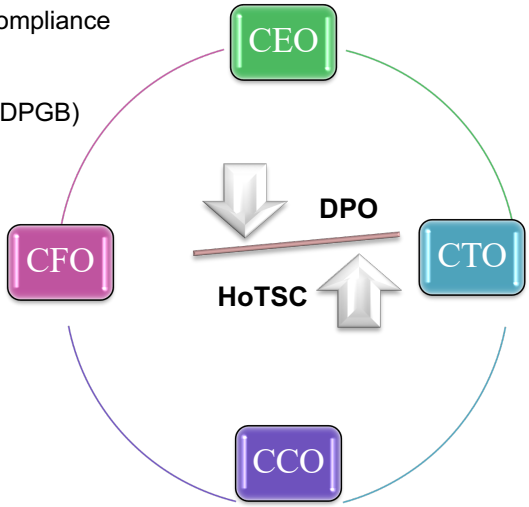
versus

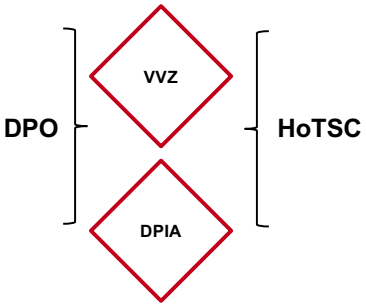
Datenschutz ist Verpflichtung des Unternehmens und Holschuld des Unternehmens beim DSB

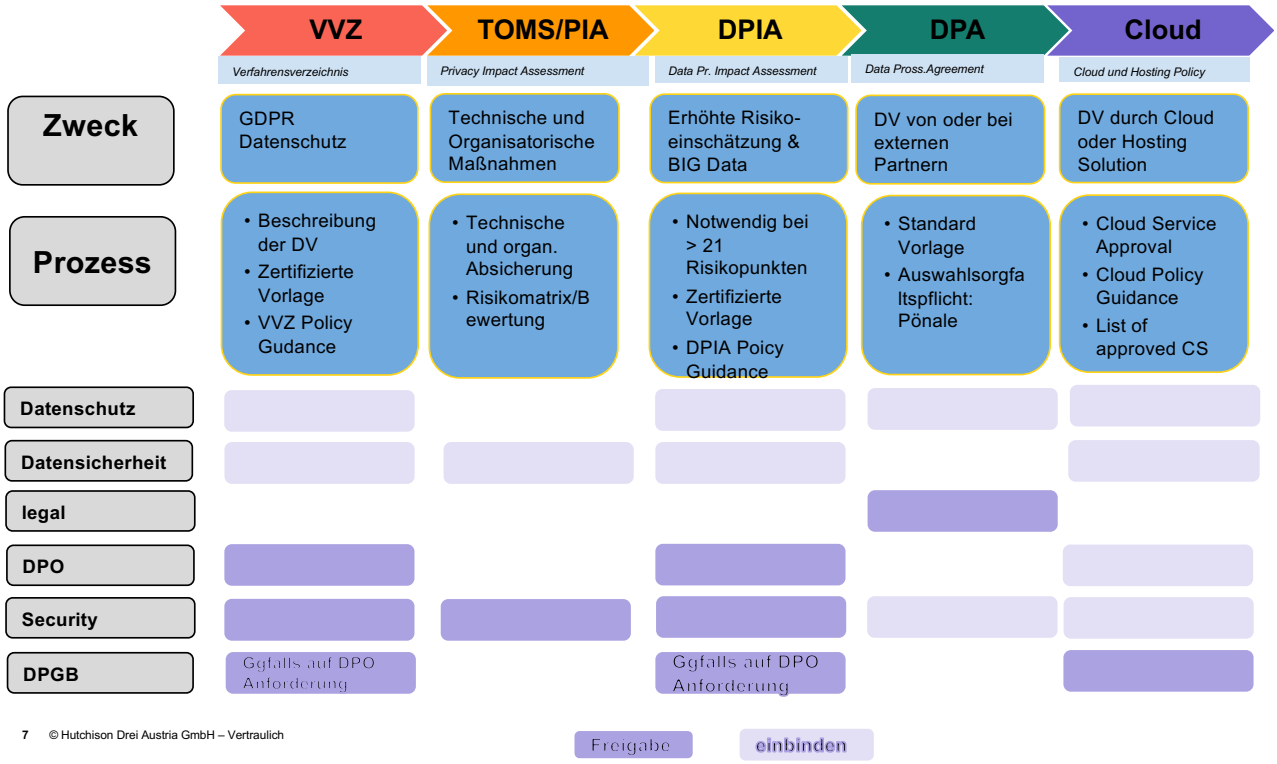
Spannungsfeld im betrieblichen Alltag

Datenschutzpositionen @Drei

- Datenschutzbeauftragte
- Head of Technical und Security Compliance
- Legal Department
- Data Privacy Governance Board (DPGB)
- Oberstes Management







Betroffene interessieren sich

- **Umfangreiche** Datenschutzerklärung
- Unterscheide Vertragsnehmer von tatsächlichem Nutzer einer Rufnummer
- Die meisten **Anfragen** von Kunden zu Beginn**: ist TelKo Auftragsverarbeiter**?
- Datensicherheit ist ein Thema, zB Ist SMS noch sicher?
- Wunsch nach **Löschung sämtlicher Daten**
- 4 Beschwerdeverfahren bei der DSB
- 1 Bescheid der DSB mit Feststellung einer Verletzung
- ISPA Code of Conduct sehr hilfreich

Kommunikationstools (E-Mail)

Interne eMail Kommunikation	Externe eMail Kommunikation
• Drei versendet interne E-Mails verschlüsselt. • Vorzugsweise immer Tools verwenden, die die Bearbeitung von Anfragen mit personenbezogenen Daten in einer Datenbank dokumentieren und festhalten (Ticketsysteme, etc.). In diesem Fall sollte man nur die Ticketnummer per E-Mail weiterverschicken. • Oft reicht es auch nur den Sachverhalt kurz darzustellen und es müssen gar keine personenbezogenen Daten erwähnt werden. • Wird eine E-Mail mit personenbezogenen Daten nicht mehr gebraucht, ist diese in der Inbox und den Sent Items zu löschen	• Drei unterstützt verschlüsselte eMail Kommunikation. Ob die E-Mail „end to end" – verschlüsselt verschickt wurde, hängt auch vom dritten Sender bzw. Empfänger ab. • Heikle Information dürfen nur dann per E-Mail kommuniziert werden, wenn diese end to end verschlüsselt übermittelt werden. • Ist das nicht möglich, so kann auch die 3BusinessCloud oder eine andere sichere Übertragungsmethode wie z.B. SFTP-Server verwendet werden. • Heikle Informationen sind jedenfalls Kundenkennwörter, Bankdaten und sonstige Daten von Zahlungsmitteln, Informationen über Krankheiten von Mitarbeitern, etc.

Überlege, ob personenbezogene Daten (insbesondere von Kunden, Mitarbeiter/HR Angelegenheiten) notwendig enthalten sein müssen bzw. an wen diese kommuniziert werden müssen;

Datenspuren von Mitarbeitern.

- pb Informationen in Office/Collaboration Tools, zB Ersteller von Dokumenten;
- Tests mit Daten von Mitarbeitern;
- Logfiles enthalten pb Daten von Mitarbeitern;

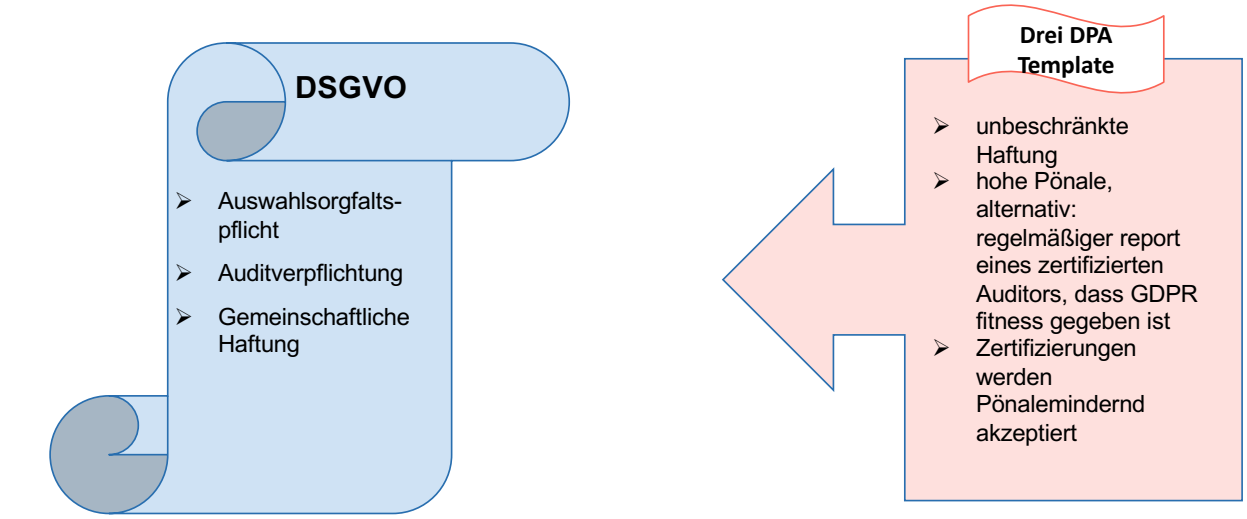
DREI definiert diese Daten als „**Company Daten**“:

- ✓ Klassifiziert als **betriebliche Informationen**
- ✓ Betroffenenrechte **eingeschränkt**
- ✓ Interessenabwägung
- ✓ In **Betriebsvereinbarungen** geregelt

Auftragsverarbeitung

Insgesamt waren im DP Programm **169** Auftragsverarbeitervereinbarungen zu prüfen/zu erstellen

Davon wurden bis dato **160** fertig abgeschlossen



Danke.

Drei. Macht's einfach.

1 Jahr DSGVO – Erste Erfahrungen und Problembereiche

IT-Rechtstag

24.05.2019

Dr. Eva Souhrada-Kirchmayer

Beschwerde gegen Bescheide der Datenschutzbehörde und bei Säumnis

Art. 78 DSGVO anwendbar

- Bescheidbeschwerden gegen Bescheide der DSB, (Säumnis-)Beschwerden bei „Untätigkeit“ der DSB
- Erster Fall des Art. 78 Abs. 2 DSGVO wird als die „herkömmliche“ Säumnis (Nichtentscheidung binnen 6 Monaten ab Beschwerdeeinbringung) gesehen
- Zweiter Fall des Art. 78 Abs. 2 DSGVO: neu, wenn Information über den Stand bzw. das Ergebnis des Verfahrens nicht innerhalb von drei Monaten von 3 Monaten erfolgt

Judikatur nach dem 25.05.2018

- BVwG entscheidet anhängige Altfälle nach der neuen Rechtslage
- Ausnahme: Zuständigkeit

Zuständigkeit der DSB

- W211 2170023-1/6E vom 21.09.2018 (siehe auch W101 2187447-1/7E vom 12.04.2019, enthält auch Überlegungen zur neuen Rechtslage)
- Ermittlungen durch StA gegen BF, Einstellung der Ermittlungen, in Akten befinden sich USB-Sticks mit personenbezogenen Daten des BF, die im Zusammenhang mit dessen anwaltlicher Tätigkeit gespeichert wurden → BF verlangte Löschung. Dem Begehren wurde nicht entsprochen.
- Beschwerde an DSB → Zurückweisung der Beschwerde (StA im Dienste der Gerichtsbarkeit tätig)
- Beschwerde des BF an BVwG → Abweisung
- O. Rev. des BF an VwGH

Judikatur zum Recht auf Geheimhaltung

Verwendung der Sozialversicherungsnummer in der Geschäftszahl

W211 2161456-1/4E vom 11.06.2018

- Behörde verwendete SV-Nr. im Rahmen einer Geschäftszahl auf Rsa- und Rsb-Rückscheinen und auf dem Kuvert von Zustellungen
- Beschwerde an DSB → Stattgebung (gesetzliche Ermächtigung für die Verwendung der Sozialversicherungsnummer als allgemeine Geschäftszahl des Rechtsträgers war nicht gegeben)
- Beschwerde der Behörde bei BVwG → Abweisung, o. Rev. zugelassen

Weiterleitung eines Mails an Personalvertreter

W253 2140428-1/9E vom 01.10.2018

- Schreiben eines Magistratsbediensteten , der selbst Personalvertreter ist betreffend Abgeltung von Fahrtkosten und Zurverfügungstellen eines Diensthandys
- Antwort der AL erging cc an drei andere Personalvertreter
- Beschwerde an DSB → Abweisung
- Beschwerde des BF an BVwG → Stattgebung (Berufung auf Art. 6 DSGVO)
- Ao. Amtsrevision an VwGH (unzutreffende Anwendung der neuen Rechtslage der DSGVO)
- Gibt es diesbezüglich eine Diskrepanz zwischen alter und neuer Rechtsordnung?

Publikation von Disziplinarerkenntnissen I

W214 2196879-1/11E vom 27.09.2018

- Ursprünglicher BF: Mitglied der Jägerschaft, dessen Disziplinarstrafe personenbezogen sowohl in einer Zeitschrift als auch auf der Website veröffentlicht wurde, auch unter Bezugnahme auf eine Verwaltungsstrafbestimmung
- Statuten sehen Veröffentlichung vor; Jägerschaft fungierte auch als Herausgeber einer Zeitschrift
- Stattgebung durch die DSB (überschießend, auch nicht von § 8 Abs. 4 DSG 2000 gedeckt)

Publikation von Disziplinarerkenntnissen II

- X-Jägerschaft: Beschwerde an das BVwG, berief sich auf das Medienprivileg
- Neue Rechtslage inzwischen anwendbar
- BVwG: Medienprivileg nicht anwendbar; X-Jägerschaft handelt im eigenen Wirkungsbereich; es handelt sich um eine Zweckänderung; Statuten sind keine gesetzliche Ermächtigung, es ist auch keine Deckung in Art. 6 und 10 DSGVO (iVm § 4 Abs. 3 DSG) gegeben.

  → Abweisung
- Keine Revision dagegen erhoben.

Weitergabe von Patientenkarteien an eine andere Ärztin I

W258 2201288-1/10E vom 03.04.2019

- Arzt ging in Pension, übergab seine Patientenkarteien an eine andere Ärztin in der Nähe, informierte per Aushang seine Patienten.
- Beschwerde eines Einschreiters nach § 30 DSG (alt), Einstellung
- Amtswegiges Verfahren → **Bescheid**: 1. Feststellung, dass das amtswegige Prüfverfahren berechtigt war und dass der Arzt die bP in ihrem Recht auf Geheimhaltung verletzt hat; 2. Arzt hat Patientenkarteien der gesetzlich zuständigen Kassenplanstellennachfolgerin binnen 14 Tagen bei sonstiger Exekution zu übergeben; 3. Ärztin hat alle Daten binnen 14 Tagen bei sonstiger Exekution restlos zu löschen und dem Arzt die Patientenkarteien zurückzustellen.

Weitergabe von Patientenkarteien an eine andere Ärztin II

- Arzt und Ärztin beschwerten sich beim BVwG
- BVwG: tw. Folge gegeben, Spruchpunkt 2 ersatzlos behoben, Spruchteil 1 und 2 neu formuliert:

„1. Es wird festgestellt, dass Dr. X, indem er am 01.10.2017 15.444 Patientenkarteien an Dr. Y. übermittelt hat, die in ihnen erfassten Patienten im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten verletzt hat.

2. Dr. Y hat binnen 14 Tagen bei sonstiger Exekution die in Spruchpunkt 1. genannten Karteien an Dr. X zurückzustellen und im Anschluss zu löschen."

Säumnisbeschwerde

W214 2196366-2/6E vom 27.09.2018

- § 30-Verfahren gegen Sachverständigen – Foto des BF wurde in ein Gutachten aufgenommen, obwohl er nichts mit dem Unfall zu tun hatte, SV war beim DVR nicht gemeldet
- wollte § 31-Verfahren – bescheidmäßige Erledigung
- Schreiben der DSB mit Hinweis auf die Nichtzuständigkeit der DSB wurde nicht zugestellt
- Säumnisbeschwerde des BF an BVwG
- Stattgebung des BVwG, Setzung einer Frist unter Äußerung einer Rechtsansicht bezüglich Sachverständiger
- Amtsrevision der DSB
- VwGH Ra 2018/04/0194-3 vom 22.03.2019, Zurückweisung der Revision

Judikatur zum Recht auf Auskunft

Verweigerung der Auskunft durch eine Rechtsanwaltskanzlei

W214 2127449-1/12E vom 27.09.2018

- BF wollte bei RA Auskunft über die ihn gespeicherten Daten (vergangener Streit mit seinem Arbeitgeber), bezieht sich auch speziell auf Kontaktdaten (da er diesbezüglich eine Löschung verlangte, aber nie eine Antwort bekommen hat)
- RA berief sich pauschal auf die in § 9 RAO normierte Verschwiegenheitspflicht und verweigerte Auskunft, leugnete Auftraggebereigenschaft
- Beschwerde an DSB → Stattgebung, Auftrag an RA, Auskunft zu erteilen
- Beschwerde der RA-Kanzlei an BVwG → Abweisung
- Beschwerde der RA-Kanzlei an VfGH, Zurückziehung der verfahrenseinleitenden Anträge durch mP → Einstellung

Auskunftserteilung von Bankdaten I

W211 2188383-1/9E vom 10.12.2018

- BF stellte ein Auskunftsbegehren über sämtliche seiner Daten, die seine Bank an eine Hausverwaltung weitergeleitet habe. Er erhielt eine Auskunft. Diese war zum Teil (z.B. hinsichtlich der Verpflichtungen nach dem Kapitalabflussgesetz und der verpflichtenden Meldungen im Rahmen von FATCA) sowie einiger Verarbeitungszwecke allgemein gehalten. Empfänger innerhalb der Bank und Kontobewegungen wurden nicht beauskunftet.
- BF beschwerte sich bei der DSB → Abweisung der Beschwerde

Auskunftserteilung von Bankdaten II

- Beschwerde an BVwG: tw. Stattgebung (hinsichtlich der allgemein gehaltenen Informationen und Verarbeitungszwecke sowie der Kontobewegungen), im Übrigen Abweisung (hinsichtlich de Verarbeitungszweckes „Vertragserfüllung“ und der „akzessorischen“ Leistungen zum Kerngeschäft Bankwesen)
- O. Rev. zugelassen
- O. Rev. von der mP (Bank) erhoben

Judikatur zum Recht auf Löschung

(keine) Löschung erkennungsdienstlicher Daten

W258 2192861-1/5E vom 03.07.2018

- A. war verdächtig, einen Porsche beschädigt und andere Personen mit einem Messer bedroht zu haben, er wurde erkennungsdienstlich behandelt
- Das Verfahren wurde durch Diversion beendet.
- Die Löschung der erkennungsdienstlichen Daten wurde von der LPD verweigert.
- Beschwerde des A. bei der DSB → tw. Stattgebung (bezüglich DNA-Daten)
- Beschwerde der LPD gegen diesen Spruchpunkt
- Beschwerdevorentscheidung der DSB – Stattgebung
- BVwG- Bestätigung der Stattgebung
- Keine Revision dagegen erhoben

(keine) Löschung von Daten durch BMI

W214 2199361-1/14E vom 19.12.2018

- BF ersuchte zunächst um Auskunft – bekam Auskunft über ein Mail über ihn, das vom BVT an ein LVT übermittelt wurde, weiters über ein Schreiben an alle LVT, in dem empfohlen wurde, den BF nicht mehr als Dolmetscher heranzuziehen, weil er einer gefährlichen Gruppierung nahestand.
- BF verlangte Löschung des Mails → BMI nahm Löschung des Mails (samt Benachrichtigung des damaligen Empfängers) vor, nicht aber des Schreibens an alle LVT (weil es nicht auf dem Mail beruhe, sondern auf anderen Ermittlungen).
- Beschwerde an DSB → Abweisung
- Beschwerde an BVwG → weitere Ermittlungen →Abweisung
- Beschwerde an VfGH

Neue Befugnisse

Anweisungsbefugnis gem. Art. 58 Abs. 2 lit. d I

- § 30-Verfahren – BF wollte anonym bleiben, Verwendung von GPS-Daten durch den Arbeitgeber zur Kontrolle von Arbeitnehmern, Arbeitgeber verwendete Einwilligungserklärungen
- Wirksamwerden der DSGVO – amtswegiges Verfahren
- Bescheid der DSB:
  - Feststellung, dass die Einwilligungserkärung nicht freiwillig erfolgte
  - Auftrag, binnen 4 Wochen bei sonstiger Exekution die Verarbeitungen in Einklang mit der DSGVO zu bringen
  - In der Begründung: allfällige Rechtmäßigkeit auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO war nicht von DSB zu überprüfen

Anweisungsbefugnis gem. Art. 58 Abs. 2 lit. d II

- Beschwerde an BVwG
- DSB: Gegenstand des Verfahrens war (nur) die Überprüfung der Einwilligungserklärung
- BVwG: (ersatzlose) Behebung, weil DSB im konkreten Fall nicht zuständig war, eine Anweisung nach Art. 58 Abs. 2 lit. d DSGVO zu erlassen (dafür war der Verfahrensgegenstand zu eng definiert)
- Ao. Amtsrevision erhoben

Fazit

- Verfahren werden zahlreicher
- Einige Strafverfahren sind eingelangt
- Noch keine internationalen Verfahren
- Hat man in der DSGVO auf eine Zusammenarbeit der Gerichte vergessen (siehe insb. Art. 60 DSGVO)?
- Weitere Entwicklung der Anwendung von Art. 79 DSGVO?

→ Kommt das „dicke Ende“ noch?

Danke für Ihre Aufmerksamkeit!

Gibt es noch Fragen?

dsb
Republik Österreich
Datenschutz
behörde

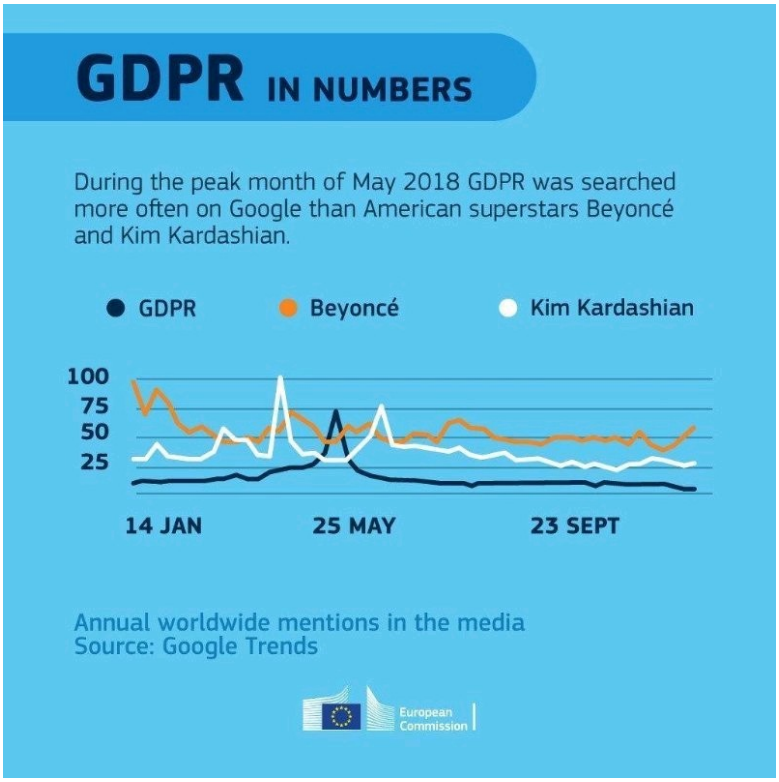
1 Jahr DSGVO – Spruchpraxis der Datenschutzbehörde

13. Österreichischer IT-Rechtstag

24.5.2019

Mag. Andreas Zavadil

dsb
Republik Österreich
Datenschutz
behörde



www.dsb.gv.at dsb@dsb.gv.at

DSGVO stärkt die DSB

Statistik 25. Mai 2018 bis dato

Art	
Beschwerden/Eingaben	**1969** (davon 241 international)
Amtswegige Prüfverfahren	**164**
Verwaltungsstrafverfahren	**189**
Anträge Verhaltensregeln	**11**
Rechtsauskünfte	**4625**

dsb
Republik Österreich
Datenschutz behörde

Spruchpraxis

Besondere Fragen 1

dsb
Republik Österreich
Datenschutz behörde

- **Subjektive Rechte nach der DSGVO und § 1 DSG – nur Kapitel III?** (Bescheid vom 30.11.2018, DSB-D122.931/0003-DSB/2018)
- **Der DSGVO ist ein Grundrecht auf Datenschutz inhärent, welches gestützt auf Art. 77 Abs. 1 DSGVO geltend gemacht werden kann, Grundsätze nach Art. 5 und 6 können daher als behauptete Verletzung von Art. 8 Abs. 1 EU-GRC geltend gemacht werden (Horizontalwirkung)** (Bescheid vom 7.3.2019, DSB-D130.033/0003-DSB/2019)

Besondere Fragen 2

- **Anweisung an Allergie-Tagesklinik; Umarbeitung der Einwilligungserklärung, Datenschutzerklärung; Bestellung eines Datenschutzbeauftragten** (DSB-D213.692/0001-DSB/2018, Bescheid vom 16.11.218, rechtskräftig)
- **Onlinepostings; Medienprivileg für Bürgerjournalismus; keine Zuständigkeit der DSB** (DSB-D123.077/0003-DSB/2018, Bescheid vom 13.8.2018, rechtskräftig)

Besondere Fragen 3

- **SVNR ist kein sensibles Datum** (Bescheid vom 9.4.2019, DSB-D123.526/0001-DSB/2019)

Rechtsschutz 1

- **Unmittelbarer Zugang zu Gericht auf Basis von Art. 79** (OGH 20.12.2018, 6 Ob 131/18k)
- **Bei identem Beschwerdegegenstand und Beschwerdegegner ist kein paralleler (d.h. zeitgleicher) Rechtsbehelf bei Aufsichtsbehörde und Gericht möglich (Art. 77, Art. 79)** (Bescheid vom 4.1.2019, DSB-D123.264/0007-DSB/2018, nicht rechtskräftig)

Rechtsschutz 2

- **Leistungsauftrag gegen einen Verantwortlichen des öffentlichen Bereichs, Einschränkung nach § 24 Abs. 5 DSG auf Verantwortliche des privaten Bereichs bleibt unangewendet (Anwendungsvorrang)** (Bescheid vom 6.6.2018, DSB-D122.829/0003-DSB/2018)
- **DSB zuständig für Beschwerden gegen Datenverarbeitungen durch StA, StA keine Gerichte oder unabhängige Justizbehörden iSv Art. 45 Abs. 2 DSRL-PJ** (Bescheid vom 16.10.2018, D123.461/0004-DSB/2018, nicht rechtskräfig)

Geheimhaltung/Freiwilligkeit 1

- **Keine Verletzung im Recht auf Geheimhaltung durch Einwilligung in Cookie-Verwendung bei Besuch der Website einer Zeitung** (Bescheid vom 30.11.2018, DSB-D122.931/0003-DSB/2018)
- **GPS-Überwachung von Unternehmens-KFZ; Anpassung der Rechtsgrundlage; keine Freiwilligkeit** (Bescheid vom 8.8.2018, DSB-D213.658/0002-DSB/2018, nicht rechtskräftig)

Geheimhaltung/Freiwilligkeit 2

- **Juristische Person, Videoüberwachung, keine Verletzung im Recht auf Geheimhaltung** (Bescheid vom 13.9.2018, DSB-D216.713/0006-DSB/2018)

Auskunft 1

- **Auskunft über Kontobewegungen; Verhältnis zu anderen Auskunfts- und Einsichtsrechten** (Bescheid vom 21.6.2018, DSB-D122.844/0006-DSB/2018, nicht rechtskräftig)
- **Kein Recht auf Feststellung, dass Auskunft verspätet erteilt wurde** (Bescheid vom 26.11.2018, DSB-D123.223/0007-DSB/2018, rechtskräftig)

Auskunft 2

- **Keine Zulässigkeit von Bestimmungen in der Datenschutzerklärung, einen Antrag auf Auskunft an eine bestimmte Adresse übermitteln zu müssen** (Bescheid vom 22.2.2019, DSB-D124.098/0002-DSB/2019)
- **Bewertung der Bonität durch Kreditauskunftei als automatisierte Entscheidung** (Bescheid vom 13.5.2019, DSB-D123.688/0003-DSB/2018, nicht rechtskräftig)

Löschung/Berichtigung 1

- **Überschießende Löschung aus Datenbank einer Kreditauskunftei und Antrag auf Berichtung** (Bescheid vom 5.12.2018, DSB-D123.211/0004-DSB/2018, nicht rechtskräftig)
- **Anonymisierung als Mittel zur Löschung** (Bescheid vom 5.12.2018, DSB-D123.270/0009-DSB/2018, rechtskräftig)

Löschung/Berichtigung 2

- **Löschfrist für negative Zahlungsdaten in Datenbank einer Kreditauskunftei; Abgehen von Rsp der DSK** (Bescheid vom 7.12.2018, DSB-D123.193/0003-DSB/2018, nicht rechtskräftig)
- **Veröffentlichung von Daten eines Arztes auf einer Bewertungsplattform im Internet; Abweisung** (Bescheid vom 15.1.2019, DSB-D123.527/0004-DSB/2018)

Löschung/Berichtigung 3

- **Speicherung von Bewerberdaten bis Ablauf der sechsmonatigen Frist nach dem GlBG (Ersatzanspruch)** (Bescheid vom 27.8.2018, DSB-D123.085/0003-DSB/2018, rechtskräftig)

Verwaltungsstrafverfahren

- **Unzulässige VÜ durch den Betreiber eines Glücksspiellokals; Strafe: EUR 4.800,00** (DSB-D550.038/0003-DSB/2018, Straferkenntnis vom 12.09.2018, nicht rechtskräftig)
- **Unzulässige VÜ durch den Betreiber eines Kebabstandes; Strafe: 1.800,00 EUR** (DSB-D550.048/0004-DSB/2018, Straferkenntnis vom 18.10.2018, nicht rechtskräftig)
- **Verwendung einer Dashcam; Strafe: 300,00 EUR** (DSB-D550.084/0002-DSB/2018, Straferkenntnis vom 27.09.2018, nicht rechtskräftig)

Verwaltungsstrafverfahren

Republik Österreich
Datenschutzbehörde

- **Verwendung einer Übersichtskamera** (DSB-D550.033/0004-DSB/2018, Ermahnung vom 13.11.2018)
- **Verdeckte VÜ über einen Zeitraum von 15 Monaten durch einen Berufsdetektiv; Strafe: 6.700,00 EUR** (DSB-D550.025/0001-DSB/2019, Straferkenntnis vom 19.2.2019, nicht rechtskräftig)

Der Externe Datenschutz-beauftragte – Ausgewählte Probleme

WOLF THEISS

13. Österreichischer IT-Rechtstag

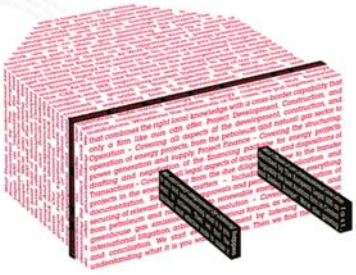
Wien, 24.05.2019

Roland Marko

WOLF THEISS

TOPICS

I. Rechtsgrundlagen
II. Zahlen
III. Ausgewählte Problemfelder



RECHTSGRUNDLAGEN

WOLF THEISS

WOLF THEISS

I. Rechtsgrundlagen

- DSGVO sieht teilweise Bestellungspflichten von Datenschutzbeauftragten (Data Protection Officers, DPOs) vor
- Rechtsgrundlagen
  - Art 37 ff Datenschutz-Grundverordnung (DSGVO)
  - § 5 Datenschutzgesetz (DSG)
  - „Leitlinien in Bezug auf Datenschutzbeauftragte“ (Opinion 243 Art 29 des Europäischen Datenschutzausschusses (EDSA), WP 243 rev.01)
- Obligatorischer oder fakultativer DPO
- Bußgelder von bis zu €10 Mio / 2% (Art 83 Abs 4 lit a; zuletzt DSB-D213.692/0001-DSB/2018)

WOLF THEISS

I. Rechtsgrundlagen

- Bestellung zum DPO
  - als „*Beschäftigter*“ des Verantwortlichen oder Auftragsverarbeiters
  - „*auf der Grundlage eines Dienstleistungsvertrags*“

  → Möglichkeit zur **Externalisierug der Funktion des DPO** (Art 37(6) DSGVO; WP 243)
- Ausnahme: Im Wirkungsbereich der Bundesministerien hat der DPO dem Dienststand des jeweiligen Bundesministeriums bzw einer nachgeordneten Dienststelle oder sonstigen Einrichtung anzugehören (§ 5(4) DSG)
- Externer DPO
  - Natürliche Person
  - Juristische Person (WP 243)

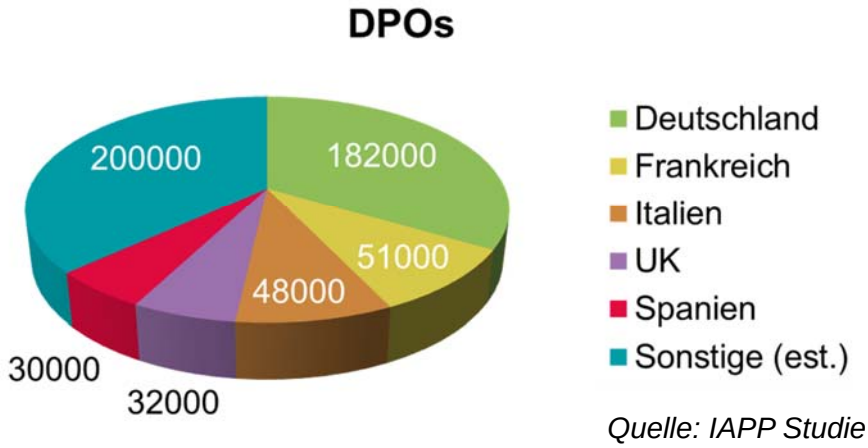
WOLF THEISS

ZAHLEN

WOLF THEISS

II. Zahlen

- ca. 500.000 bestellte DPOs in EU-Mitgliedstaaten (öffentl./privat)



Quelle: IAPP Studie 2019

- Beispiel Frankreich:
  - ca. 50.000 Datenschutzbeauftragte
  - ca. 18.000 externe Datenschutzbeauftragte

PROBLEMFELDER

WOLF THEISS

WOLF THEISS

III. Rollen- und Berufsbild

- Aufgaben des DPO in Art 39(1) DSGVO geregelt
- Doppelrolle des DPO
  - Berater in allen Datenschutzangelegenheiten für Management und Mitarbeiter
  - Zusammenarbeit mit und Anlaufstelle für die Aufsichtsbehörde
- „Mittler zwischen den maßgeblichen Interessenträgern“ (EDSA)
  - Aufsichtsbehörde
  - betroffene Personen
  - Geschäftsführung

WOLF THEISS

III. Rollen- und Berufsbild

- Keine positivierte Regelung der beruflichen Qualifikation in DSGVO
- Erfahrung im nationalen und europäischen Datenschutzrecht und „umfassendes Verständnis“ der DSGVO (WP 243)
- Wohl hA: Rechtliche, technische und organisatorische Kenntnisse, dh
  - Verstehen der jeweiligen durchgeführten Verarbeitungsvorgänge
  - Kenntnisse im Bereich der IT und Datensicherheit
  - Kenntnis der jeweiligen Branche und Einrichtung
- Je komplexer die Datenverarbeitungsvorgänge/Umfang, desto höher die Anforderungen an die Fachkompetenz des DPO
- Individuelle Kenntnisse und Fähigkeiten von Mitarbeitern der Organisation des externen DPO können einander ergänzen

WOLF THEISS

III. Rollen- und Berufsbild

- DSGVO behält die Ausübung der Funktion eines externen DPOs keiner bestimmten Berufsgruppe vor
- DPO-Aufgaben umfassen u.a. auch die *Vertretung vor der Aufsichtsbehörde* → Vertretungsmonopol der Rechtsanwälte?
- *Sachlich begrenzte* Parteienvertretungsbefugnisse können sich aus sonstigen gesetzlichen Bestimmungen ergeben (§ 8(3) RAO, zB Unternehmensberater, Baumeister, Immobilienmakler)
- § 136 Abs 3 Z 3 GewO idgF erlaubt Unternehmensberatern die Vertretung vor Behörden und Körperschaften öffentlichen Rechts
- Berufsbild der Unternehmensberater und IT-Dienstleister schließt nach wohl hA die Funktion des externen DPO ein
- Restrisiko?

11

WOLF THEISS

III. Unabhängig & weisungsfrei

- Ausübung der Tätigkeit in Unabhängigkeit und Weisungsfreiheit für DPO Mitarbeiter und Externe gewährleistet
- Entscheidungsbefugnis und Verantwortlichkeit bleibt jedoch bei Verantwortlichem / Auftragsverarbeiter
- DPO sollte in dem Fall einer Entscheidung gegen seine Empfehlung das Management konsultieren und dokumentieren
- Keine Abberufung oder Benachteiligung aufgrund der Ausübung der Funktion → Problem bei externen DPOs durch (Androhung der) Kündigung des Dienstleistungsvertrages?
- EDSA-Empfehlung: Bestellung externer DPOs mit Mindestlaufzeit von 2 Jahren
- Kündigungsschutz von Mitarbeitern des externen DPO?

12

WOLF THEISS

III. Interessenskonflikte

- Konfliktsituationen, wenn der externe DPO Gefahr läuft
  - sich selbst zu überwachen,
  - seine eigene Arbeitsleistung zu überprüfen und
  - dieses gegebenenfalls zu kritisieren hätte
- Mögliche Beispiele:
  - Wirtschaftliches Interesse am Unternehmenserfolg (zB Gesellschafter)
  - Beratungstätigkeit des Unternehmens, die mit Datenschutz in Spannungsverhältnis steht (zB Inkaufnahme von Risiken oder Ressourcenschonung im Datenschutz)
  - Vertretung in streitigen Datenschutzangelegenheiten

WOLF THEISS

III. Interessenskonflikte

- Externer DPO – und auch alle Mitglieder der zum DPO bestellten Organisation – dürfen keinem Interessenskonflikt unterliegen
- Empfehlung des EDSA zur Vermeidung von Interessenskonflikten bei einzelnen Mitarbeitern durch
  - Zentrale Aufgabenverteilung durch Kontaktperson beim DPO und
  - gezielte interne Trennung der Aufgabenbereiche (Chinese Wall)
- Wichtig: Dokumentation, wonach ggf trotz Verdachtslage *kein* Interessenskonflikt vorliegt

WOLF THEISS

III. Haftung

- Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche oder der Auftragsverarbeiter verantwortlich, der sicherzustellen und nachzuweisen hat, dass Verarbeitung DSGVO-konform erfolgt
- DPO ist im Fall der Nichteinhaltung der Datenschutzanforderungen nicht persönlich verantwortlich
- Beraterhaftung bei externem DPO?
- Kein Regressnahme für auferlegte Bußgelder
- Versicherung

WOLF THEISS

Danke für Ihre Aufmerksamkeit!

WOLF THEISS

Kontakt

RA Mag. Roland Marko, LL.M.
Wolf Theiss Rechtsanwälte
Tel: (+ 43 1) 515 10 5880
e-mail: roland.marko@wolftheiss.com

Datenschutzrechtliche Implikationen des CLOUD Act für Europa

13. IT-Rechtstag

25.4.2018

Axel Anderl, Nino Tlapak

DORDA

WE DELIVER CLARITY.

WE DELIVER CLARITY. INFOLAW WWW.INFOLAW.AT DORDA

Agenda

- ☐ Hintergrund zum CLOUD Act
- ☐ Inhalt und Anwendungsbereich des CLOUD Act
- ☐ Datenschutzrechtliche Implikationen
- ☐ CLOUD Act in der Praxis
- ☐ Vertragliche Lösungsansätze

Hintergrund zur Entwicklung des CLOUD Act

Zugriff auf Daten durch US-Behörden

- eingeschränkter Zugriff durch **Patriot Act**
  - Sec 215 US Patriot Act iVm § 1861 des FISA
  - Zugriff für US Sicherheitsbehörden
  - zu Zwecken der Spionage- und Terrorismusabwehr
  - auf Geschäftsunterlagen aller Art ("*any tangible things*") → also auch **Daten**
  - von jeder beliebigen Stelle
  - fraglich: Exterritorialität?
    - Zugriff auch auf Daten, die außerhalb der USA gespeichert sind, möglich?

WE DELIVER CLARITY. INFOLAW WWW.INFOLAW.AT DORDA

Hintergrund zur Entwicklung des CLOUD Act

Zugriff auf Daten durch US-Behörden

- umfangreicher Zugriff durch **Stored Communications Act** (SCA)
  - 18 U.S.C. § 2701ff (seit 1986 in Kraft)
  - Zugriff durch gerichtliche Anordnung (court order)
  - Zur Aufklärung jeder Straftat (keine Mindeststrafe)
  - auf sämtliche erforderliche Informationen → also auch **Daten**
  - von Anbietern von elektronischen Kommunikationsdiensten (zB E-Mail) und Remote-Computing-Diensten (zB Cloud)
  - fraglich: Exterritorialität?
    - Zugriff auch auf Daten, die außerhalb der USA gespeichert sind, möglich?

Hintergrund zur Entwicklung des CLOUD Act

Zugriff auf Daten durch US-Behörden

- Anlassfall: Microsoft vs USA (Supreme Court)
  - US-Behörden verlangen Zugriff auf E-Mail Account wegen Drogendelikt
  - Account ist bei Microsoft Irland gespeichert
  - Microsoft Irland lehnt Zugriff ab
  - US-Behörde klagt Zugriffsrecht ein
  - Microsoft gewinnt in zwei Instanzen → Frage an US Supreme Court
- Zentrales Thema: Exterritorialität
  - Können US-Behörden nach SCA auf Daten außerhalb der USA zugreifen?
- Wende: wenige Wochen vor dem Urteil wird CLOUD Act erlassen
  - Supreme Court Entscheidung damit obsolet

CLOUD Act – Inhalt und Anwendungsbereich

Wesentliche Bestimmungen

- Kernbestimmung: 18 U.S.C. § 2713

A provider of electronic communication service or remote computing service shall (…) ***disclose*** *the contents of a wire or electronic* ***communication*** *and* ***any record or other information*** *pertaining to a customer or subscriber within such provider's* ***possession, custody, or control****,* ***regardless of whether such communication, record, or other information is located within or outside of the United States****.*

CLOUD Act – Inhalt und Anwendungsbereich

Wesentliche Bestimmungen

- Kernbestimmung: 18 U.S.C. § 2713
  - Anbieter eines elektronischen Kommunikationsdienstes oder von Remote-Computer-Diensten müssen
  - Inhalte von drahtgebundenen oder elektronischen Nachrichten, alle Aufzeichnungen oder andere Informationen, die sich auf einen Kunden oder Abonnenten beziehen, die
  - in Besitz, in Verwahrung oder sonst unter der Kontrolle des Anbieters
  - aufbewahren, sichern und offenlegen
  - unabhängig davon, ob sich diese innerhalb oder außerhalb der USA befinden

WE DELIVER CLARITY. INFOLAW WWW.INFOLAW.AT DORDA

CLOUD Act – Inhalt und Anwendungsbereich

Persönlicher Anwendungsbereich

- alle Anbieter, die "*der Gerichtsbarkeit der USA unterworfen sind*"
  - Gesellschaften, die nach amerikanischem Recht gegründet wurden, oder
  - durch eine solche beherrscht oder besessen werden
    - damit auch Tochtergesellschaften von US Müttern erfasst, sofern beherrscht oder besessen

→ Alle US-Anbieter und deren Tochtergesellschaften

CLOUD Act – Inhalt und Anwendungsbereich

Sachlicher Anwendungsbereich

- alle Daten, die sich in "*Aufbewahrung, unter der Kontrolle oder im Besitz eines Anbieters befinden*"
  - faktischer Zugang oder das Recht, diese Daten zu erlangen, ausreichend
- alle Informationen für "*aktuelle polizeiliche Untersuchungen*"
  - anders als bei "FISA" ist der Datenzugriff nicht auf terroristische Angriffe oder Spionageaktivitäten beschränkt
  - sämtliche Straftaten denkbar, unabhängig von der Strafhöhe

  → weiter Anwendungsbereich!

CLOUD Act – Inhalt und Anwendungsbereich

Fehlende (direkte) Rechtsbehelfe

- standardmäßig eingeschränkter Rechtsschutz für nicht US Bürger
  - Rechtsbehelfe nur für den dem gesetz unterliegenden (Cloud-)Provider
  - kein direkter Rechtsschutz für Betroffene in EU
- Aber: US Regierung kann (bilateral) Abkommen zur Erweiterung Rechtsschutz abschließen (18 U.S.C. § 2523)
  - kann weitere Bedingungen, Beschränkungen oder Zugriffsverbote auf Daten, die sich im Ausland befinden, vorsehen
  - weiterer Rechtsschutz (direkter Betroffenenschutz) möglich
  - auch ausländischen Behörden kann Auskunftsrecht an US Konzerne gewährt werden (Reziprozität)
  - bislang keine Abkommen geschlossen!

Datenschutzrechtliche Implikationen

CLOUD Act und DSGVO – ein Widerspruch?

- Datenübermittlung an einen EU-Anbieter einer US-Mutter ✔
  - Auftragsverarbeitervereinbarung (Art 28 DSGVO)

- Datenübermittlung an einen US-Anbieter ✔
  - Auftragsverarbeitervereinbarung (Art 28) und
  - geeignete Garantien (Art 46)
    - Standardvertragsklauseln; oder
    - Angemesseneheit durch EU-US Privacy Shield; oder
    - Genehmigung der Datenschutzbehörde

Datenschutzrechtliche Implikationen

CLOUD Act und DSGVO – ein Widerspruch?

- Offenlegung persönlicher Daten an US-Behörden ✗
  - keine Lösung über Auftragsverarbeitung, da kein Zweck des Cloud-Nutzers als Verantwortlicher (Cloud-Anbieter = Normadressat)
  - US CLOUD Act keine rechtliche Verpflichtung iSd Art 6 Abs 1 lit c DSGVO
    - da weder nationales noch Unionsrecht
  - Übermittlung/Offenlegung an Gerichte/Behörden aus Drittstaaten nur aufgrund internationaler Abkommen (Art 48 DSGVO) zulässig
    - bisher gibt es aber (noch) keine solche Vereinbarung!
- Dilemma für Cloud Anbieter
  - Herausgabe = Verstoß gegen DSGVO
  - Verweigerung = Verstoß gegen CLOUD Act

CLOUD Act in der Praxis

Keine offiziellen Richtlinien oder Stellungnahmen

- keine Informationen oder Stellungnahmen österreichischer Behörden
- keine (deutliche) Erklärung der EU-Kommission
  - trotz parlamentarischer Anfragen im Juli 2018
  - trotz Antrag des EU-Parlaments auf Suspendierung des Privacy Shields
  - finale EBA Guidelines on Outsourcing sprechen US CLOUD Act nicht an
- geplante Verhandlungen zwischen der EU Kommission und dem US Government zu potentiellem bilateralen Abkommen ab Juni 2019

➔ *Die Offenlegung von Daten an US-Behörden ist eine höchstpolitische Angelegenheit!*

CLOUD Act in der Praxis

Gegenmaßnahmen/Strategie der EU?

- aktuelle Agenda der EU-Kommission
  - bereits Verhandlungen mit den USA
    - über den Zugriff auf elektronische Beweise in US Clouds
    - zu den erforderlichen Rechtsbehelfen
  - Start der Gespräche: Juni 2019

- E-Evidence Verordnung als Gegengewicht?
  - Erleichterung polizeilicher Abfragen persönlicher Daten
  - durch EU und MS Behörden
  - für Straftaten mit mehr als drei Jahren Strafdrohung

CLOUD Act in der Praxis

Gegenmaßnahmen/Strategie der EU?

- Anwendungsbereich E-Evidence Verordnung:
  - Provider, die in EU-MS Kommunikationsdienste anbieten
    - daher auch für Anbieter aus dem Drittland
  - nach Sicherungsanordnung: Datenkopie anlegen
  - nach Herausgabeanordnung: Übermittlung an Behörden
    - Teilnehmerdaten (Name, Geburtsdatum, Postanschrift, Telefonnummer)
    - Zugangsdaten (Datum und Uhrzeit der Nutzung, IP-Adresse)
    - Transaktionsdaten (Sende- und Empfangsdaten, Standort des Geräts, verwendetes Protokoll) sowie
    - Inhaltsdaten

CLOUD Act in der Praxis

Zugriffe durch US-Behörden in der Praxis

- US Behörden bislang sehr zurückhaltend bei Anfragen im Ausland
  - Allerdings: Statistiken betreffen Zeitraum vor Klärung Zugriffsmöglichkeit
- inhaltlich üblicherweise nur Kontostammdaten verlangt
  - Wer ist der Nutzer?
  - dR keine Inhaltsdaten angefragt
- bislang meist nur natürliche Personen betroffen
  - Unternehmen nur in Ausnahmefällen
  - wenn Unternehmen, dann Terrorabwehr
- faktische terrotiriale Einschränkung, wegen US-Bezug Straftat

Vertragliche Lösungsansätze

Schutzmaßnahmen gegen CLOUD Act

- vertragliche Überbindung rechtlicher Verpflichtungen auf den Cloud-Anbieter
  - insbesondere behördliche Regelungen und EBA-Richtlinien
  - Bankgeheimnis
- strenge Geheimhaltungs- und Vertraulichkeitsregelungen
  - unter Berücksichtigung branchenspezifischer Besonderheiten, insbesondere im Banken und Versicherungsbereich
- Vereinbarung umfassender (Daten-)Sicherheitsmaßnahmen
  - zB Verschlüsselung und Pseudonymisierung
  - Wenn Daten nicht zugänglich sind/Provider keinen Schlüssel hat, wird das Risiko minimiert!

Vertragliche Lösungsansätze

Schutzmaßnahmen in Cloud-Verträgen

- Informationspflichten für Anbieter, wenn eine US-Behörde Datenzugriff verlangt
  - Vorsicht, teilwiese Gag-Order (Info unzulässig) möglich
- Pflicht des Anbieters, Rechtsmittel gegen Herausgabeanordungen voll auszuschöpfen
  - Kunden Äußerungsmöglichkeiten geben
  - Informationsaustausch und laufende Updates
- rasche Beendigungsmöglichkeit des Vertrages
  - kurze Kündigungsfristen
  - ggfs Recht zur Kündigung aus wichtigem Grund bei Änderung der rechtlichen Rahmenbedingungen

Ansprechpartner

Dr Axel Anderl, LL.M.

- Managing-Partner bei DORDA
- Absolvent der Universität Wien (Dr iur 2005) und des Universitätslehrgangs für Informationsrecht und Rechtsinformation der Universität Wien(IT-Law) (LL.M. 2001)
- Fachliche Schwerpunkte: IT-Recht, insb E-Commerce, Datenschutzrecht, Urheber-, Medien- und Wettbewerbsrecht
- ILO Clients Choice Award für E-Commerce 2012 und 2013
- ILO Clients Choice Award für Information Technology 2014, 2015, 2016, 2017, 2018 und 2019
- Empfohlen als leading individual sowohl in IT als auch IP recht bei legal500;
- führender Anwalt in IT-Recht bei “Chambers Europe”,
- Legal500 Hall of Fame für TMT
- Autor zahlreicher Fachpublikationen in den Bereichen IT-, Urheber- und Medienrecht
- Vortragender Donau Universität Krems ("Datenschutz und Privacy"), Universität Wien (IT-Rechtslehrgang) und Universität Innsbruck (Digitalisierung)
- Co-Chair Technology Sourcing Committee von ITechLaw

WE DELIVER CLARITY. INFOLAW WWW.INFOLAW.AT DORDA

Ansprechpartner

Mag Nino Tlapak, LL.M.

- Rechtsanwalt bei DORDA
- Universität Wien, Mag iur 2012
- Universität Wien, Universitätslehrgang Medien- und Informationsrecht, LL.M. (IT-Law) 2013
- Fachliche Schwerpunkte: Datenschutzrecht, IT-Recht, E-Commerce, Outsourcing, Urheber- und Medienrecht
- Empfohlen als Next Generation Lawyer im Bereich TMT im renommierten internationalen Handbuch "Legal 500“
- Autor von Fachpublikationen im Bereich Datenschutz und E-Commerce
- Vortragender für Datenschutzrecht bei den Master-Lehrgängen "Digital Business" an der FH Technikum Wien sowie "Technisches Management" an der FH Campus Wien, Donau Universität Krems ("Datenschutz und Privacy")
- Mitglied der Interessensgemeinschaften "www.it-law.at" und "Privacyofficers.at"

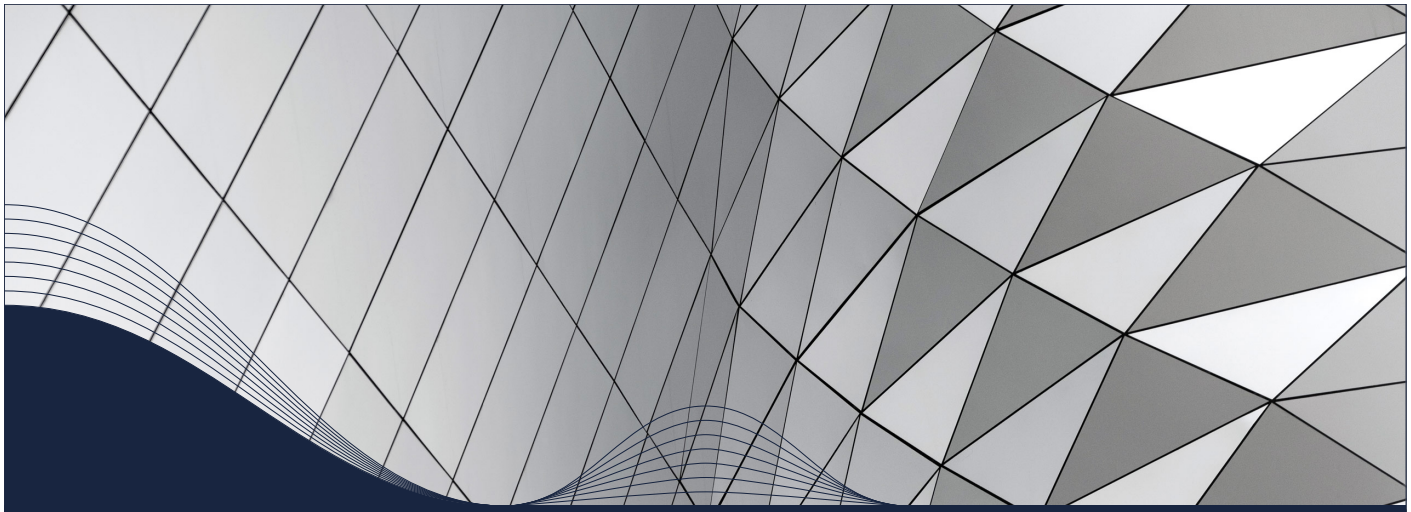
Kontakt

Dr Axel Anderl, LLM
T: +43 1 533 47 95 – 23
E: axel.anderl@dorda.at

Mag Nino Tlapak, LLM
T: +43 1 533 47 95 – 23
E: nino.tlapak@dorda.at

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien

International Law Office - Information Technology Award for Austria 2014, 2015, 2016, 2017, 2018 & 2019
International Law Office - E-Commerce Award for Austria 2012 & 2013
JUVE - Austrian Law Firm of the Year 2017



Datenschutzrechtliche Anforderungen an betriebliche Kommunikationsmittel

13. Österreichischer IT-Rechtstag

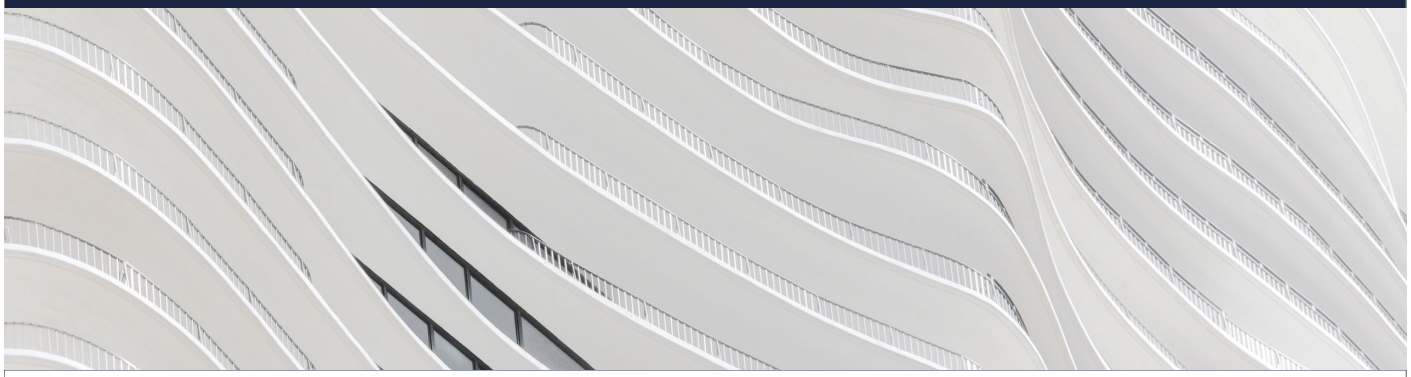
Mag. Stefan Panic

DLA PIPER

Themenübersicht

- Grundsätzliche Anforderungen – Anwendungsfälle der DSGVO
- Problembereiche bei betrieblicher E-Mail Kommunikation
  - Einsichtsrechte des Arbeitgebers
  - Aufbewahrung und Löschung
  - Betroffenenrechte
- Neue Kommunikationsmittel

Grundsätzliche Anforderungen



Grundsätzliche Anforderungen und Anwendungsfälle

Datenverarbeitung bei Kommunikationsmitteln

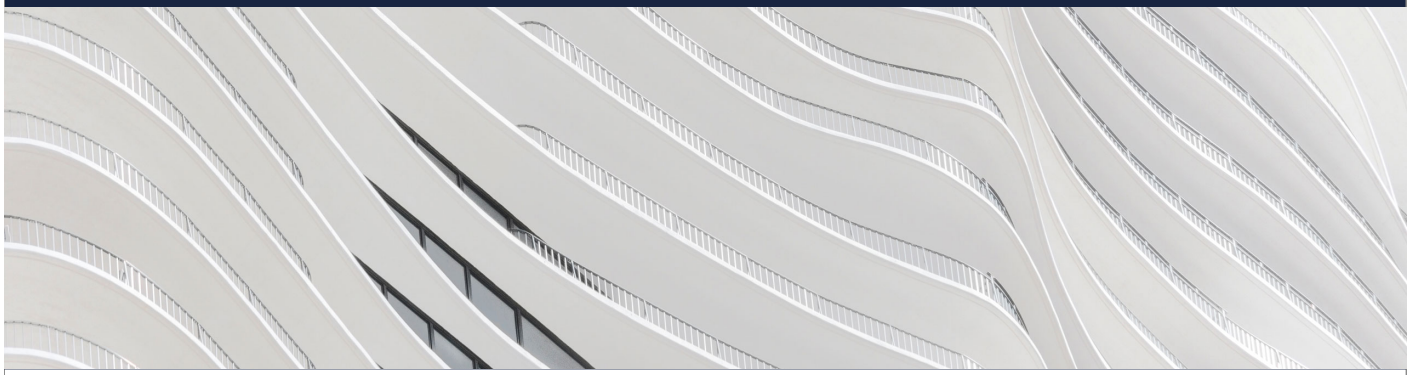
- Elektronische Datenverarbeitung bei Kommunikation – v.a. bei Emails und ähnlichen Kommunikationsmitteln
  - SMS, interne und externe Messenger Dienste, auch VoIP
- Verkehrsdaten (Email Adressen, Telefonnummern) und Inhaltsdaten
- Erfordernisse im Überblick
  - Rechtsgrundlagen nach Art 6 – 9 DSGVO
    - idR Vertragserfüllung (lit b) oder berechtigte Interessen (lit f)
  - Einhaltung angemessener Datensicherheitsmaßnahmen
  - Bei Auslagerung (zB von Email Servers) – ADV Verträge und ggf Rechtsgrundlagen nach Kapitel V hinsichtlich Übermittlung in Drittländer
  - Verzeichnis der Verarbeitungstätigkeiten

Grundsätzliche Anforderungen und Anwendungsfälle

Verschlüsselung

- Müssen E-Mails verschlüsselt sein?
- Allgemeine Anforderung an Datensicherheit – Art 32 Abs 1 a) DSGVO
  - Allerdings "unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos"
- Keine spezifische Verpflichtung für Kommunikation
  - Erforderlich oder empfehlenswert bei sensibleren Berufen aufgrund spezifischer Vorgaben (zB Gesundheitsdienstleister)
- Viele E-Mail-Server sind ohnehin verschlüsselt

Betriebliche E-Mail Kommunikation – Problembereiche



Durchsicht von E-Mails / Kommunikation

Allgemeines

- Unterschiedliche Fallsituationen und Umstände
  - Geschäftsbezogene Einsichtnahme vs andere Gründe
  - Durchsicht im Einzelfall vs umfassende Auswertung
  - *ex post* vs *ex ante*
  - Private Kommunikation vs berufliche Kommunikation
- Keine ausschließlich datenschutzrechtliche Problematik
  - Recht auf Privatsphäre (Art 8 EMRK)
  - Telekommunikationsgeheimnis (§ 93 TKG 2003, § 119 StGB)
  - Mitarbeiterkontrolle (§§ 96ff ArbVG)
  - Sonderregeln im öffentlich-rechtlichen Bereich (§§ 79c-79i BDG)

Durchsicht von E-Mails / Kommunikation

Zulässiger Bereich

- Speicherung von Kommunikation zwecks ihrer Durchführung
  - Teil des gewöhnlichen Wirtschaftsbetriebes
  - Rechtsmäßig gemäß Art 6 Abs 1 lit b DSGVO
- *Ex post* Durchsicht geschäftlicher Kommunikation im Einzelfall für die Geschäftsabwicklung
  - Ebenso für den Betrieb unerlässlich
- Automatische Kontrolle, insb der eingehenden Kommunikation, zwecks Schadenprävention
  - Antiviren, Spam-Filter uä
  - Wohl / in aller Regel durch berechtigte Interessen des Unternehmens, Schaden von der IT Infrastruktur abzuwenden, zu rechtfertigen (Art 6 Abs 1 lit f DSGVO)

Durchsicht von E-Mails / Kommunikation

Kommunikationskontrolle – problematische Bereiche – Untersuchungen (I)

- Auswertung der (geschäftlichen) Kommunikation aus anderen Gründen als Geschäftsabwicklung
  - iaR wegen Verdacht von strafbaren Handlungen und/oder Vertragsverletzung
  - Mögliche Rechtsgrundlage – berechtigte Interessen
    - Auch im Fall strafbarer Handlungen - § 4 Abs 3 Z 2 DSG
    - Vorliegen von sensiblen Daten? (= private Kommunikation?) → berechtigte Interessen nicht anwendbar; Möglichkeit einer Einwilligung?
  - Massenauswertung – Konflikt mit dem Datenminimierungsprinzip (Art 5 Abs 1 lit c DSGVO)
- Einwilligung als Lösungsmöglichkeit
  - Wirksamkeit
  - Kooperationsbereitschaft
  - Wer müsste einwilligen (→ mehrere Kommunikationspartner)?

Durchsicht von E-Mails / Kommunikation

Kommunikationskontrolle – problematische Bereiche – Untersuchungen (II)

- Folgeproblem – Datenübermittlung an Gerichte und Behörden
  - Berechtigte Interessen oder rechtliche Verpflichtung (Art 6 Abs 1 lit c DSGVO)
  - Heranziehung des Art 9 Abs 2 lit f DSGVO – Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
    - Analoge Anwendung bei Daten, die nicht unter Art 9 fallen?
  - Weiteres Konfliktpotential mit dem Datenminimierungsgrundsatz – was ist für das Verfahren relevant?
- Ausländische Verfahren (insb USA)
  - rechtliche Verpflichtung nicht anwendbar! ("SWIFT" Stellungnahme der Art 29 WP – WP 128)
    - Übertragbarkeit der Argumentation auf Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen? Verhältnis mit Art 49 Abs 1 lit e DSGVO?
  - Berechtigte Interessen – Umfang?
- Einwilligung als "letzter Ausweg"?

Durchsicht von E-Mails / Kommunikation

Kommunikationskontrolle – problematische Bereiche – systematische Kontrolle

- Automatische Kontrolle ohne Verdachtsmomente, insb auch bezogen auf den Inhalt
  - "Data Loss Prevention" Systeme
  - Problematisch auch bei geschäftlicher Kommunikation, insb mangels jeglicher Verdachtsmomente
    - Verhältnismäßigkeit und Datenminimierung
- Zulässigkeit umstritten und einzelfallabhängig – eine Folgeabschätzung jedenfalls empfohlen
- Lösungsansätze
  - "stufenweise Kontrollverdichtung"
  - Minimierung des Eingriffes durch Ausgestaltung des Systems
    - Mitarbeiterselbstbestimmung – Mitarbeiter wird als erster über einen möglichen "Trigger" informiert
    - Beteiligung des Betriebsrates

Durchsicht von E-Mails / Kommunikation

Problemfeld Privatnutzung

- Strengere Regeln im Bereich privater Kommunikation
- Nach hA – Einsichtnahme in private Kommunikation grds jedenfalls untersagt (Telekommunikationsgeheimnis)
  - Ausnahmen in besonders gravierenden Fällen (rechtfertigender / entschuldigender Notstand)?
- Auswirkung auf Durchsicht und Kontrolle im Allgemeinen
  - Trennung zwischen privater und geschäftlicher Kommunikation oft schwierig
- ZT von der Zulässigkeit der Privatnutzung abhängig – drei Varianten
  - Privatnutzung erlaubt
  - Privatnutzung untersagt
  - Keine Regelung

Durchsicht von E-Mails / Kommunikation

Problemfeld Privatnutzung – Varianten

- Erlaubte Privatnutzung
  - Potentielle Eingriffsmöglichkeit höher
  - Vorkehrungen müssen getroffen werden, dass keine Einsicht in private Kommunikation erfolgt
- Untersagte Privatnutzung
  - Grds keine Erwartung der Privatheit
  - Allerdings ist auch in diesem Fall die Durchsicht privater Kommunikation grds unzulässig (EGMR RS *Bărbulescu/Rumänien)*
  - Keine Vorkehrungen notwendig, aber sofortiges Unterlassen beim Erkennen privater Kommunikation
- Keine Regelung
  - Wohl von einer eingeschränkten Zulässigkeit der Privatnutzung auszugehen
  - Somit ist striktere Herangehensweise empfohlen

Aufbewahrung und Löschung

Aufrechtes Dienstverhältnis

- Spannungsverhältnis – Aufbewahrungspflichten <> Löschungsrecht / Datenminimierungspflicht
- Allgemeine Aufbewahrungsdauer?
  - Jedenfalls 7 Jahre bei geschäftlichen E-Mails - §§ 132 BAO, 212 UGB – E-Mails als Geschäftsbriefe
  - Darüber hinaus gemäß den Verjährungsfristen?
    - Wahrscheinlichkeit eines Verfahrens?
    - Bestimmung der anwendbaren Verjährungsfrist

Aufbewahrung und Löschung

Nach Ausscheiden

- Notwendigkeit des Zugriffs auf die Inboxen der ausgeschiedenen Mitarbeitern – datenschutzrechtliche Zulässigkeit
- ZT parallel zur Einsichtnahme während des aufrechten Dienstverhältnisses
  - Unterscheidung nach der Zulässigkeit der Privatnutzung
    - Einsicht im Fall der zugelassenen Privatnutzung oder erwarteten Privatnutzung mangels Regelung eingeschränkt bzw mit Einschränkungen zu versehen
  - Bei Zulässigkeit der Privatnutzung – Umgang mit allfälligen Privaten E-Mails (→ Betroffenenrechte?)

Betroffenenrechte im Zusammenhang mit E-Mails

- Geltendmachung des Auskunftsrechts über den Inhalt eines E-Mails?
- Recht auf Datenportabilität
- Datenintegrität
  - Aufbewahrungspflicht für private E-Mails nach Ausscheiden?

Neue Kommunikationsmittel

Neue Kommunikationsmittel

Ausgangslage

- In vielen Betrieben wird die Kommunikation sowohl intern als auch extern (mit Kunden, Geschäftspartnern usw.) immer mehr von gewöhnlichen Kanälen (Telefon, Email) auf Messenger-Dienste bzw Apps (WhatsApp, Facebook Messenger usw.) verschoben
- Insb WhatsApp wird in vielen Betrieben als Kommunikationsmittel benutzt
- Konsequenzen oft unklar
  - Technische Unklarheiten in Bezug auf tatsächliche Datenverarbeitung
  - Folglich rechtliche Unklarheiten

Problembereich WhatsApp

- Auslöser – (familienrechtliche) Entscheidung des Amtsgerichts Bad Hersfeld (D) (Beschl. v. 20.03.2017 - F 111/17 EASO)
  - Hauptthema Sorgerechtsverfahren / Verletzung der Sorgepflicht
  - Datenschutzrechtlicher Hintergrund – Nutzung von WhatsApp durch das minderjährige Kind führt zur Datenweitergabe an WhatsApp Inc.
    - Automatische Datenweitergabe der im Adressbuch abgespeicherten Kontaktdaten zwecks Kontaktabgleichs
    - Die Weitergabe betrifft **alle** Kontakte (sowohl WhatsApp Nutzer als auch Nichtnutzer)

Problembereich WhatsApp

Potentielle Datenschutzverletzungen der automatischen Datenweitergabe

- Fehlende Rechtsgrundlage nach Art 6 DSGVO
  - Einwilligung der Betroffenen wurde verneint, auf alle Fälle für Kontakte im Adressbuch, die den Dienst **nicht** nutzen
  - Eine konkludente Einwilligung der Kontakte, die WhatsApp nutzen, wurde aber auch verneint
  - Andere Rechtsgrundlagen wurden nicht behandelt (berechtigtes Interesse nach Art 6 Abs 1 lit f DSGVO?)
- Außerdem – fehlende Rechtsgrundlage für Übermittlung ins Drittland nach Kapitel V DSGVO
  - Wurde vom Gericht nicht analysiert
  - Inzwischen (mehrfach) überholt
    - Für europäische Nutzer kommt der Vertrag mit WhatsApp Ireland Ltd zustande
    - WhatsApp Inc inzwischen (seit 8.3.2018) Privacy Shield zertifiziert
- Unklare Nutzungsbedingungen hinsichtlich weiterer Datenverarbeitung

Ausweitung des Problembereichs

- Grundsätzliches Problem der Datenweitergabe auf andere gängige Messenger-Dienste übertragbar
  - Nutzungsbedingungen von Facebook Messenger: "*We also collect contact information if you choose to upload, sync or import it from a device […]*"
  - Nutzungsbedingungen von Viber: "*Eine Kopie der Telefonnummern und Namen aller Ihrer Kontakte (ob sie nun Viber-Mitglieder sind oder nicht – aber nur Name und Telefonnummer) wird gesammelt und auf unseren Servern gespeichert, damit wir Ihnen und Ihren Kontakten eine Verbindung ermöglichen können.*"
- Die Importierung erfolgt zT automatisch, zT muss sie vom Nutzer freigegeben werden

Lösungsansätze

Rechtliche und tatsächliche Lösungsansätze

- Untersagung des Zugriffes auf das Adressbuch
  - Praktischer Problem: Nützlichkeit stark eingeschränkt
- Einholung einer Einwilligung nach Art 6 Abs 1 lit a DSGVO
  - Praktisch schwer tunlich, selbst wenn die Kontakte auf das Notwendige eingeschränkt werden
  - Außerdem unklar, ob die Einwilligung "in informierter Weise" (iSd Art 4 Z 11 DSGVO) erfolgen würde – Unklarheiten über die Weiterverwendung der Daten durch den Betreiber
- Betreiber des Messenger Dienstes als Auftragsverarbeiter?
  - Grds denkbar – Kontaktdatenabgleich wäre ein klarer und eingeschränkter "Auftrag des Verantwortlichen"
  - Keinerlei Deckung in den jeweiligen Nutzungsbedingungen – keine Übereinstimmung mit Art 28 DSGVO, insb ist das Weisungsrecht nach Abs 3 lit a keineswegs abgebildet
  - Vereinbarung im Einzelfall äußert untunlich

Lösungsansätze

Rechtsmäßige Alternativen?

- Europäische Diensteanbieter, deren Dienste datenschutzkonform sind?
  - Fehlen der Grundlage nach Art 6 ebenfalls ein Hindernis
- Vermeidung der Übermittlung personenbezogener Daten
  - Kontaktdatenabgleich über gehashte Daten (zB App "Signal")
- Technische und rechtliche Analyse im Einzelfall empfehlenswert
  - Ob und ggf in welcher Form eine Datenweitergabe stattfindet?
  - Am Bsp von Signal – reicht das Hash-Verfahren, damit die Kontakte als anonyme Daten eingestuft werden können?

Vielen Dank für Ihre Aufmerksamkeit!

Mag. Stefan Panic
Senior Associate
T: +43 (0) 1 531 78 1034
F: +43 (0) 1 533 52 52
stefan.panic@dlapiper.com

DLA Piper Weiss-Tessbach Rechtsanwälte GmbH
Schottenring 14
A-1010 Wien, Österreich
Telefon: +43 (0)1 531 78 1451
Fax: +43 (0)1 533 52 52