

T.I.S.P. Community Meeting

Berlin, 14. - 15.11.2017

Auswirkungen der DS-GVO auf die Informationssicherheit

Mareike Gehrman

TaylorWessing Partnerschaftsgesellschaft mbB

TaylorWessing

Inhalt

- 01 > Allgemeines
- 02 > Erhöhung des Strafrahmens
- 03 > Direkte IT-Sicherheitsanforderungen nach Art. 32 DS-GVO
- 04 > „Versteckte“ Pflichten?
- 05 > Datenschutz durch Organisation und Technik
- 06 > Schutzkonzept
- 07 > Rechtsrahmen IT-Sicherheit
- 08 > Ausblick



EU-Datenschutzgrundverordnung (DS-GVO)

Idee: Ein Datenschutzgesetz für alle EU-Mitgliedstaaten mit unmittelbarer Anwendung!

- Ende der Umsetzungsfrist: 25. Mai 2018
- Art. 2: Anwendung bei der Verarbeitung von personenbezogenen Daten
- Personenbezogene Daten sind „... *alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen...*“
 - *Direkter oder indirekter Personenbezug*
 - *Bsp.: Name, Kennnummer, Standortdaten, Online-Kennung, Scoringergebnis, gehashte E-Mail Adresse, KFZ-Kennzeichen, IP-Adresse*



Ab 05/2018 wird es teurer!

Deutlich höhere Bußgelder:

- EUR 20 Mio. oder 4 % des jährlichen weltweiten Jahresumsatzes von Unternehmen / -gruppe
 - *Artt. 8, 11, 25 bis 39, 41 Abs. 4, 42, 43*
- EUR 10 Mio. oder 2 % des jährlichen weltweiten Jahresumsatzes von Unternehmen / -gruppe
 - *Artt. 5, 6, 7, 9, 12 bis 22, 44 bis 49, 58 Abs. 1, 2*

Rechtsfolgen:

- Schadensersatz
- Bußgeld
- Strafe (nach nationalem Recht)

Prozessstandschaft, Art. 80



IT-Security – Sicherheitsmaßnahmen (1)

Art. 32 DS-GVO:

„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 für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten ...“

- ▶ Aus dem Gesetzestext wird also ersichtlich, es bedarf einer Verhältnismäßigkeitsprüfung



IT-Security – Sicherheitsmaßnahmen (2)

- > Ziel: Sicherheit der Daten und der Verarbeitung durch technische und organisatorische Maßnahmen
- > Adressaten: Verantwortliche / Auftragsverarbeiter
- > Faktoren: Ergreifen von angemessenen technischen und organisatorischen Maßnahmen unter Berücksichtigung
 - des Stands der Technik
 - der Implementierungskosten
 - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
 - der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten der Betroffenen



IT-Security – Sicherheitsmaßnahmen (3)

- ▶ Aber: Faktoren sind bei der Prüfung der Verhältnismäßigkeit nur zu berücksichtigen!

- > Ausdrücklich benannte Maßnahmen nach Art. 32 DS-GVO sind :
 - Pseudonymisierung und Verschlüsselung
 - Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste
 - Rasche Wiederherstellung der Verfügbarkeit und des Zugangs zu Daten nach einem Zwischenfall
 - Regelmäßige Überprüfung der Maßnahmen, Ersetzung durch bessere, sicherere Verfahren („*Stand der Technik*“)



- Wann gilt eine Maßnahme als geeignet?
 - Eine Maßnahme ist geeignet, wenn sie das Ziel des Art. 32 DG-SVO erfüllen kann, also die Aufrechterhaltung der Sicherheit und der Vorbeugung gegen eine gegen die DS-GVO verstoßende Verarbeitung
 - Auch eine nicht rein technische Lösung kann also eine angemessene Maßnahme darstellen ► Gesetz ist technikneutral!
- Angemessen ist das Schutzniveau, wenn es die vorherig genannten Aspekte berücksichtigt und in einer dem Einzelfall entsprechenden Weise erfüllt
 - Zwingend bei der Überlegung der Angemessenheit betrachtet werden, müssen allerdings gemäß Art. 32 Abs. 2 DS-GVO die Risiken, die mit der jeweiligen Verarbeitung verbunden sind

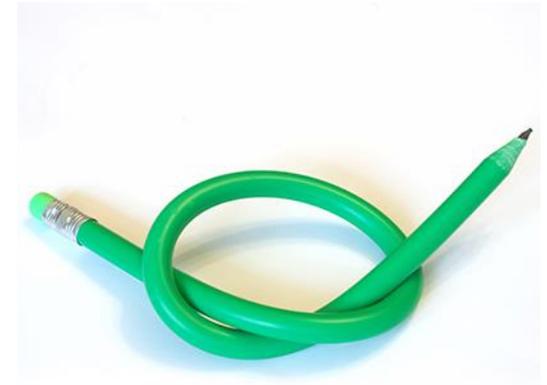


Nur Umsetzung genügt nicht: Dokumentation!

Verantwortlicher hat die Darlegungs- und Beweislast, dass die IT-Sicherheitsanforderungen eingehalten werden!

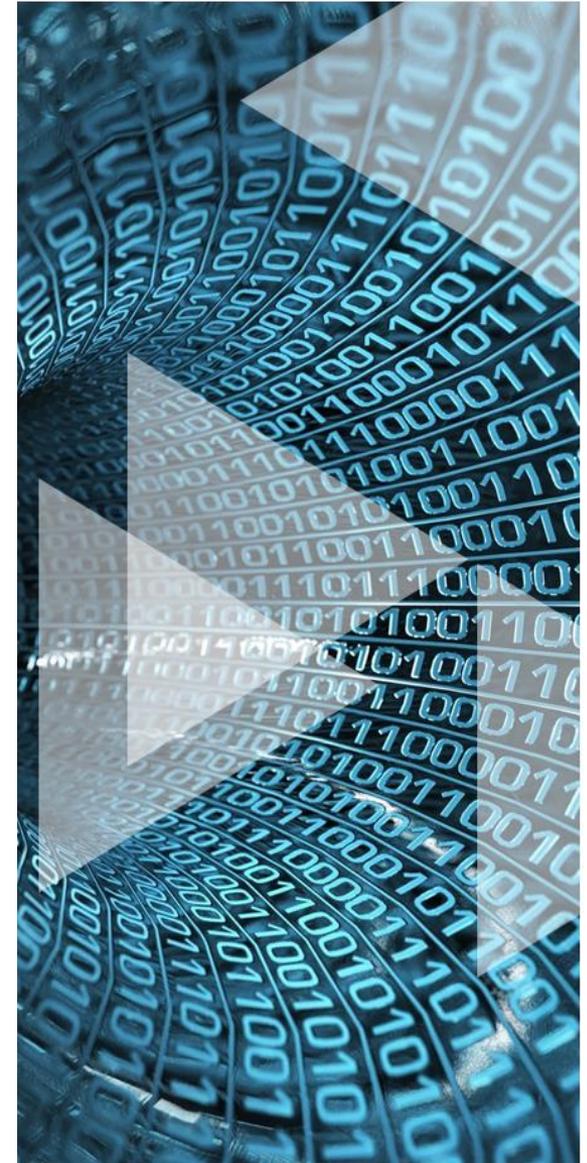
- ▶ Bitte dokumentieren Sie deshalb umfassend!
 - Positive und negative Entscheidungen
 - Alle ergriffenen Maßnahmen

„...unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken ... geeignete technische und organisatorische Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“



IT-Sicherheit ist nicht nur Art. 32 DS-GVO

- > Betroffenenrechte verpflichten ebenfalls zur Umsetzung von IT-Sicherheitsmaßnahmen
- > Löschpflicht nach Art. 17 DS-GVO
 - Art. 17 DS-GVO gewährt den Betroffenen ein Recht auf vollständige Löschung ihrer Daten. Wer also z.B. Opfer eines Hackerangriffs mit Datendiebstahl wurde, ist nicht mehr in der Lage dieses Recht auf Löschung zu gewährleisten.
- > Auskunftsrecht nach Art. 15 DS-GVO
 - Betroffenen muss über die Frage der Datenverarbeitung Auskunft erteilt werden sowie weitergehende Informationen zur Verfügung gestellt werden (z.B. Empfänger der Daten)



IT-Sicherheit ist nicht nur Art. 32 DS-GVO

- > Informationspflichten nach den Artt. 13 und 14 DS-GVO
 - Betroffene müssen über Datenerhebung informiert werden und haben Anspruch auf weitergehende Informationen wie z.B. der Verwendungszweck
- > Dasselbe gilt für die anderen Betroffenenrechte wie das Recht auf Berichtigung (Art. 16 DS-GVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) oder das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)!



Meldepflichten und IT-Sicherheit?

- > Meldung an Behörde, Art. 33 DS-GVO
 - Frist: unverzüglich, möglichst binnen 72 Stunden nach Kenntnis, Verspätung begründen
 - Inhalt: Beschreibung der Verletzung, Kontaktdaten des Datenschutzbeauftragten, Beschreibung der Folgen und ergriffenen Maßnahmen
 - Ausnahme: Voraussichtlich kein Risiko für Rechte und Freiheit der natürlichen Person
- > Benachrichtigung des Betroffenen, Art. 34 DS-GVO
 - Frist: unverzüglich
 - Form: Klare und einfache Sprache
 - Ausnahmen:
 - Kein hohes Risiko für die Rechte und Freiheiten
 - Geeignete TOMs, die eine Verarbeitung verhindern
 - Unverhältnismäßiger Aufwand (öffentliche Bekanntmachung)



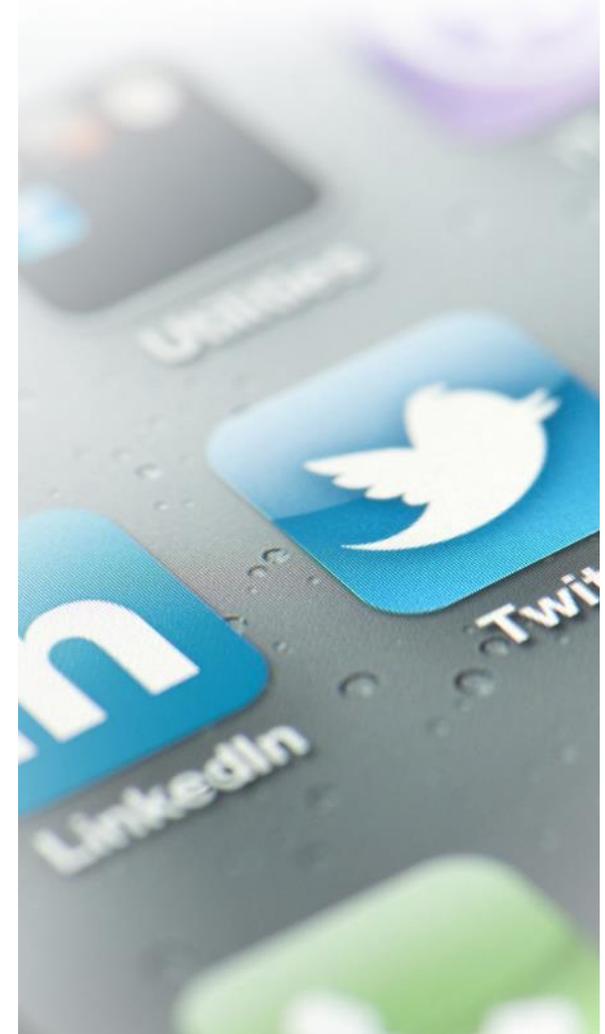
Weitere Schutzmaßnahmen

- > Welche **technischen** und **organisatorischen** Maßnahmen kennt die DS-GVO (EW 78)?
 - *Datenschutz durch Technikgestaltung*
 - *Datenschutzfreundliche Voreinstellung (z.B. App)*
 - *Minimierung von Verarbeitungsprozessen*
 - *So schnell wie möglich pseudonymisieren*
 - *Sicherheitsfunktionen*
 - *Interne Strategien*
 - *Überwachung der Verarbeitung durch Betroffenen*
 - *Softwarebeschaffungsvorgaben („Hersteller ermutigen“)*

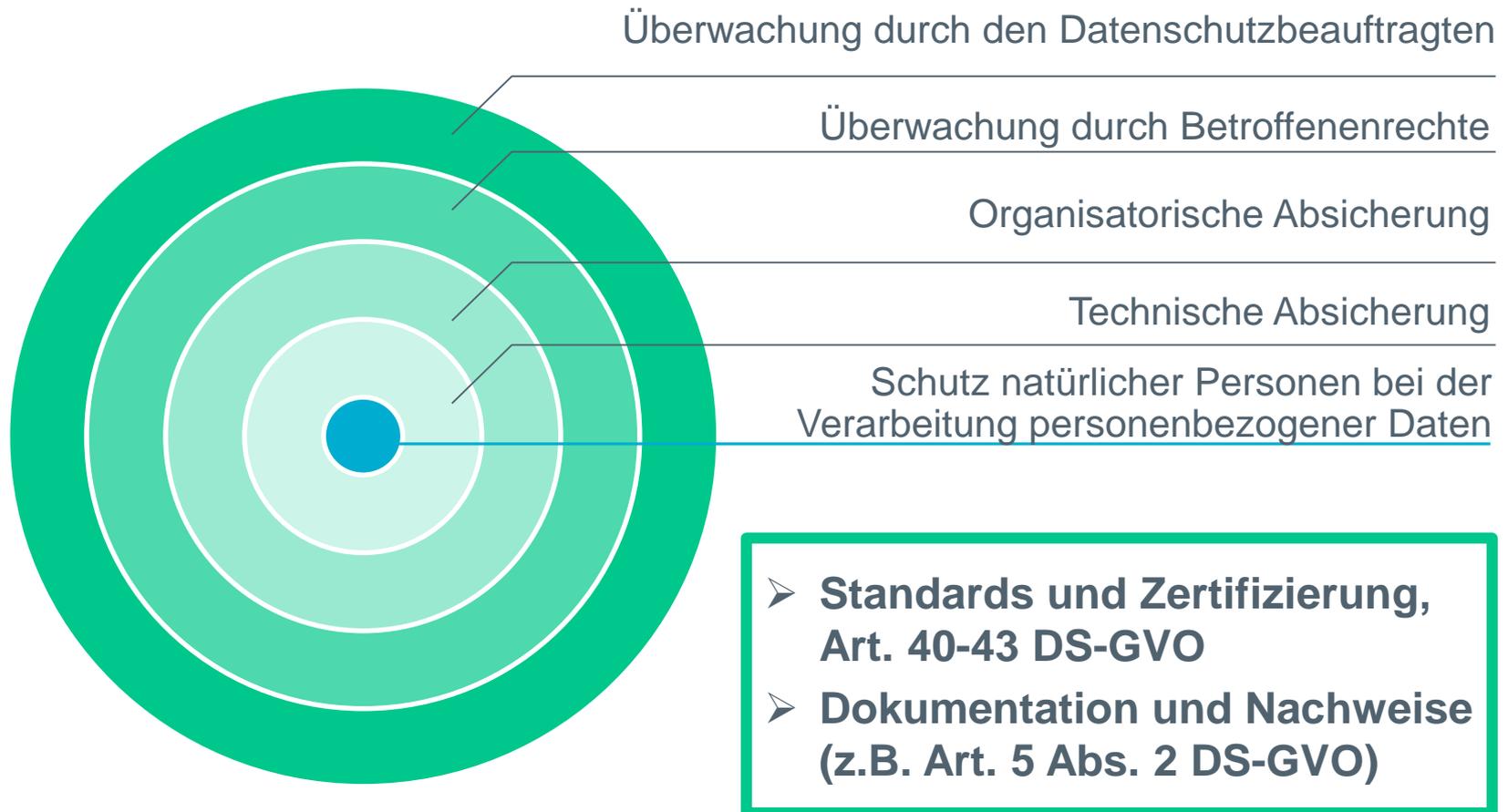


Datenschutz durch Technik

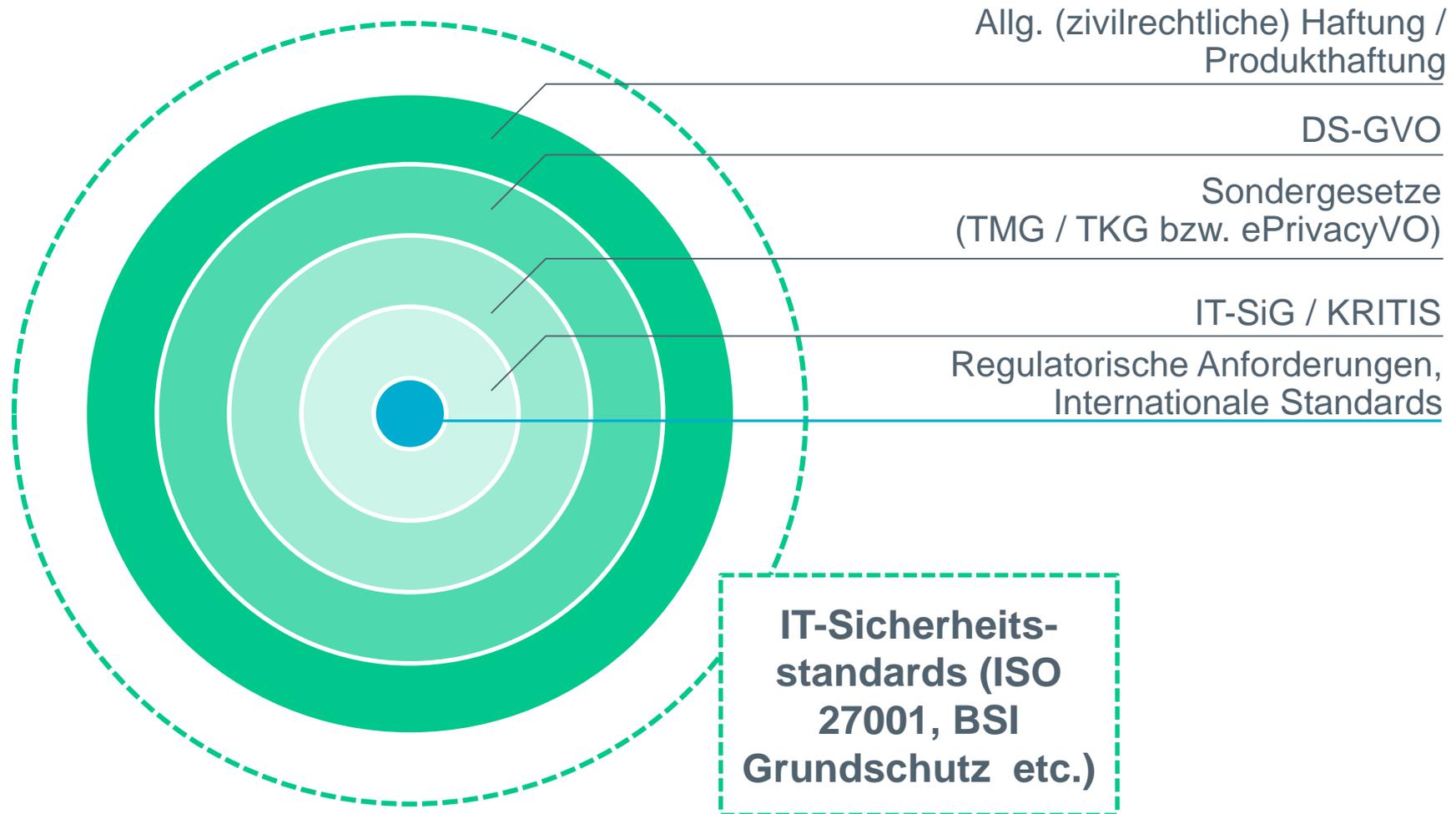
- > Privacy by Design / Default, Art. 25 DS-GVO
 - Datenschutz durch Technikgestaltung (by Design)
 - Berücksichtigung bereits bei Planung und Konzeption
 - Datenminimierung und sonstige Prinzipien
 - Technisch: Pseudonymisierung, Verschlüsselung, Hinweise, Pop-ups, Speicherbegrenzung, Funktionen zur Umsetzung der Betroffenenrechte
 - Organisatorisch: Schulung, Kontrollen, Datenschutzkonzept
 - Datenschutzfreundliche Voreinstellung (by Default)
 - Keine Pflicht zum Einsatz von Nutzerumgebungen
 - Kein „Datenvorrat“ (Zweckbindung)
 - Voreinstellung: Kleiner Empfängerkreis



Datensicherheit durch verschiedene Schutzmaßnahmen



Wie fügt sich die DS-GVO in die Gesetze zur IT-Sicherheit ein?

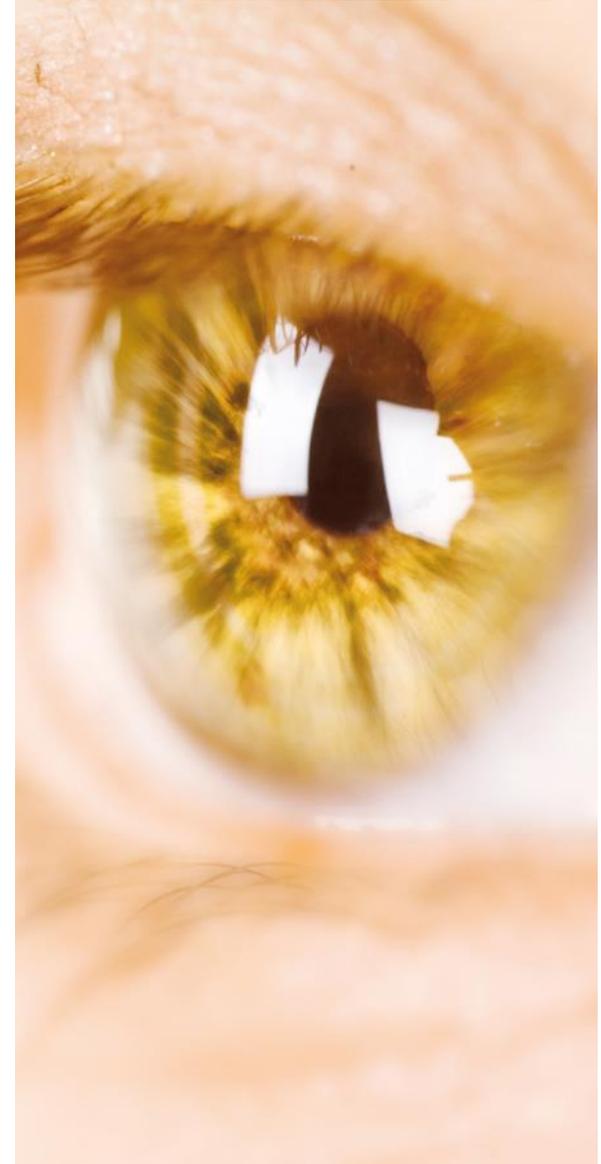


Kooperation von Recht und Technik

> Entwicklung

- Bislang setzte das europäische und deutsche Datenschutzrecht den Rahmen für Technik
- USA stellen technische Möglichkeiten in den Vordergrund und passen das Recht aktuellen Entwicklungen an
- Erste Annäherungsversuche mit Safe-Harbor Principles und EU-US Privacy-Shield
- Erneut: DS-GVO erkennt Datenschutz durch Technik (Stichwort „*Privacy by Design*“) an, DS-GVO ist dabei technikneutral
- Parallele: IT-SiG und die NIS-RL schlagen „amerikanischen Weg“ ein, z.B. Mitwirkungsrechte der Branchen

▶ Wegweisendes Umdenken oder Ausnahme?



Was ist Ihre Meinung?

Sind Fragen offen geblieben?



Ihre Ansprechpartnerin



Mareike Christine Gehrmann
Salary Partnerin, Düsseldorf
Fachanwältin für
Informationstechnologierecht

- > **Informationstechnologie/Telekommunikation**
- > **Datenschutz**
- > **Litigation & Dispute Resolution**



Mareike Christine Gehrmann hat sich auf die rechtliche Beratung in den Bereichen IT, Telekommunikation und Datenschutz spezialisiert. Sie berät nationale sowie internationale Mandanten in allen operativen Belangen zum IT-, Telekommunikations- und Datenschutzrecht. Hierbei hat Mareike Christine Gehrmann auch komplexe IT-Projekte der öffentlichen Hand, insbesondere des Bundesministerium des Innern und seiner nachgelagerten Bereiche, begleitet.

Besondere Expertise weist Mareike Christine Gehrmann in den Bereichen IT-Sourcing, Datenschutz und Cyber Security vor. Ein Schwerpunkt ihrer derzeitigen Tätigkeit ist die Implementierung der EU-Datenschutzgrundverordnung. Darüber hinaus verfügt sie über umfangreiche Erfahrungen beim Führen großer Gerichtsverfahren (bis OLG-Ebene) und DIS-Schiedsverfahren im IT- und Telekommunikations-Bereich.

Mareike Christine Gehrmann studierte Rechtswissenschaften an der Heinrich-Heine-Universität Düsseldorf. Dort nahm sie auch erfolgreich an den Begleitstudiengängen Anglo-American Law und Internetrecht teil. Während ihrer Studienzeit absolvierte sie auch ein freiwilliges Praktikum beim Deutschen Generalkonsulat in New York.

Von 2001 bis 2012 arbeitete Mareike Christine Gehrmann als freie Mitarbeiterin bei einer regionalen Tageszeitung. Seit 2015 ist sie Mitglied im Expertennetzwerk der „Computerwoche“ und veröffentlicht zu aktuellen Themen aus dem Bereich „Cybersecurity“. Zudem verfasst sie regelmäßige Beiträge in verschiedenen Fachzeitschriften und referiert zu ihren Spezialgebieten.

Im Januar 2016 wurde sie zur Fachanwältin für Informationstechnologierecht ernannt. Mareike Christine Gehrmann ist zudem sicherheitsüberprüft gemäß SÜG.

Kontakt Daten

T: +49 211 8387-189

E: m.gehrmann@taylorwessing.com

Unsere Informationen zu IT und Datenschutz

Moderne Rechtsberatung beinhaltet selbstverständlich mehr als die Begleitung von Projekten und die Prüfung einzelner Fragestellungen. Wir wollen in der Zusammenarbeit vielfältigen Mehrwert schaffen. Insbesondere im Bereich IT/IP und Datenschutz haben wir attraktive Zusatzleistungen für unsere Mandanten entwickelt.

Newsletter

Regelmäßig versenden wir unseren **Newsletter Technology**, um Sie über aktuelle juristische Themen, relevante Gesetzgebungsinitiativen oder Verfahrensergebnisse und deren Konsequenzen auf dem Laufenden zu halten.

Microsites

Unsere Microsite **Global Data Hub** enthält darüber hinaus aktuelle und detailliertere Informationen zu praxisrelevanten Fragen im internationalen Datenschutz.

Konferenzen, Workshops & Webinars

Wir bieten unseren Mandanten diverse Konferenzen, wie z.B. den **Münchener Datenschutztag** sowie Workshops und Veranstaltungen, kostenlos zur Weiterbildung und Vernetzung an. Zu ausgewählten und aktuellen juristischen Themen führen wir Webinars durch.

Global Intellectual Property Index

In unserem Global IP Index werden über 30 Rechtsordnungen aus dem gesamten Bereich des gewerblichen Rechts- und Datenschutzes verglichen, bewertet und in einer Studie zusammengefasst. Erstmals werden auch Industrieaspekte miteinbezogen. Die fünfte Auflage wird in Kürze veröffentlicht.





Unsere monatlichen Beiträge rund um IoT :

<https://deutschland.taylorwessing.com/de/internet-of-things>

TaylorWessing