Cyber Secure –
Der Kampf des Gesetzgebers

GESICHERT IN STÜRMISCHEN ZEITEN.

COLOSSEUM THEATER ESSEN

05.12.2017

Mareike Gehrmann
TaylorWessing, Rechtsanwältin

DER FACHKONGRESS FÜR DATEN-
INFORMATIONS- & IT-SICHERHEIT

TaylorWessing

„The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.”

(Eugene Howard Spafford,
Amerikanischer Professor für Informatik an der Purdue Universität und führender IT-Sicherheitsexperte)

Inhalt

01 > Gesetzeslage vor 2015

02 > Gesetzesinitiativen seit 2015

03 > Das IT-Sicherheitsgesetzes

04 > DS-GVO

05 > IT-Sicherheit in der Welt

06 > Dschungel IT-Sicherheit

06 > Resümee?

01 > Gesetzeslage vor 2015

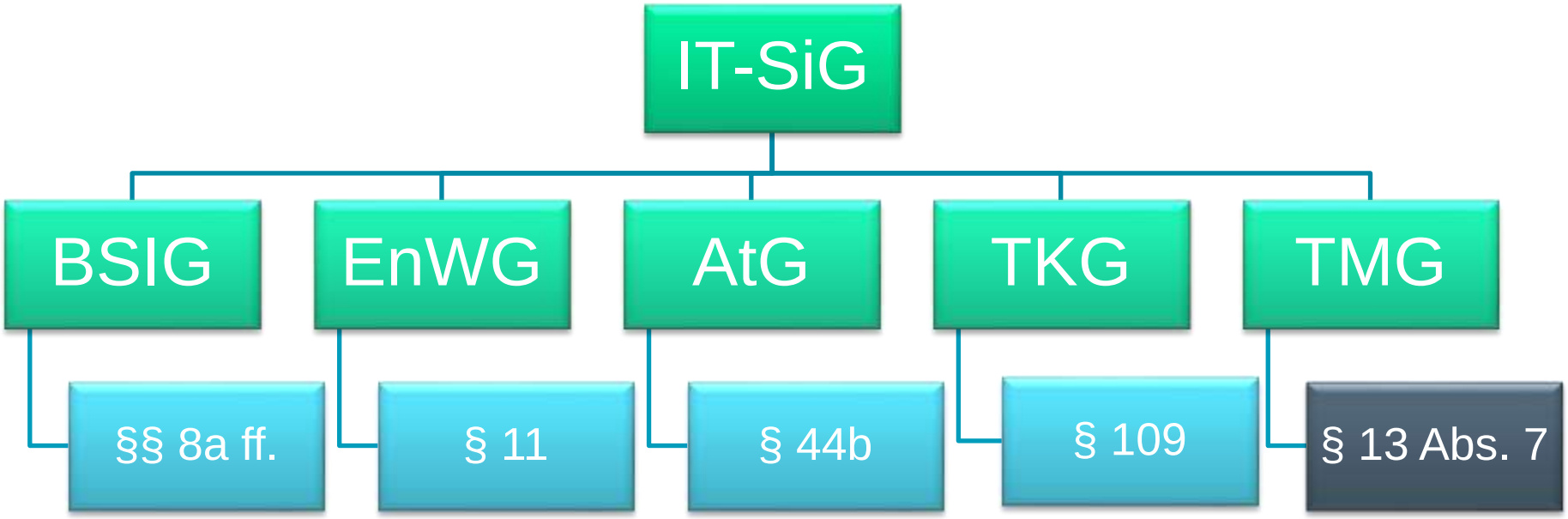
Gesellschaftsrecht § 91 Abs. 2 AktG (analog); § 111 AktG (analog); § 43 Abs. 1 GmbHG	▪ *„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“* → Sicherstellung von IT-Security als Bestandteil des **Risikomanagements**
Handelsrecht **Steuerrecht** **Revisionssicherheit**	▪ §§ 239 Abs. 4 S. 2; 257; 261 HGB; 147 AO; GoB; GoBS; GDPdU ▪ Jeder Kaufmann hat bei der Führung seiner Handelsbücher und der Aufbewahrung seiner Unterlagen in elektronischer Form die Sicherung der Systeme zu gewährleisten und seinen Aufbewahrungs- und Archivierungspflichten nachzukommen. ▪ außerdem: Mitwirkungspflicht bei Betriebsprüfungen
Bürgerliches Recht	▪ **Deliktsrecht:** Organisationsverschulden bei unzureichender IT-Sicherheit ▪ **Vertragsrecht:** Pflicht zu IT-Compliance kann sich vertraglich ergeben (z.B. vertragliche Vereinbarung von Sicherheitsstandards) ▪ Allg. rechtl. Regelungen, z.B. § 241 Abs. 2 BGB
Datenschutz Verpflichtung zu technischen und organisatorischen Schutzmaßnahmen, berufsspezifische Sondervorschriften	▪ § 9 BDSG „Acht Gebote der Datensicherheit“ ▪ §§ 113a Abs. 10, 109 Abs. 2 TKG, § 13 Abs. 4 TMG ▪ § 78a SGB X ▪ Insb. Umgang mit Kunden- und Angestelltendaten ▪ ggf. zusätzliche berufsgruppen-/ unternehmensspezifische Schutzpflichten, z.B. §§ 66 StBerG, § 51b WPO, § 25a KWG, § 33 WpHG

Der Kampf des Gesetzgebers

Entdeckung der IT-Sicherheit

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-SiG**)
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI (**BSI-KritisV**)
- Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Europäischen Union (**NIS-RL**)
- EU-Datenschutzgrundverordnung (**DS-GVO**)
- **Regulatorische** Anforderungen (z.B. VAG)
- **Internationale Standards** (z.B. Certificate of Conformity)

Beispiel: IT-Sicherheitsgesetz – Ein Gesetz viele Adressaten



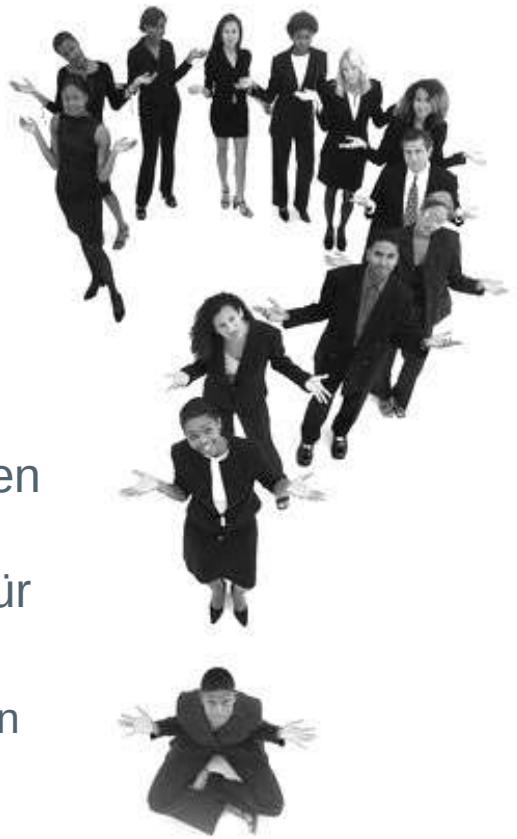
Diskutiert wird hierüber: BSI-Gesetz und NIS-Richtlinie

Eine weitere Unbekannte: Dienstleister, insb. ITK-Branche

BSIG – Die Suche nach dem Adressaten

Wann ist man KRITIS-Betreiber? KritisVO

1) Definition der Dienstleistungen in den Sektoren
   - ❖ Beispiel: Trinkwasserversorgung, Abwasserbeseitigung
2) Identifizierung der Kategorien von Anlagen, die für die Erbringung der kritischen Dienstleistungen erforderlich sind
   - ❖ Beispiel: Kanalisation, Kläranlagen, Leiteinrichtungen
3) Bestimmung der konkreten Anlagen oder Teile, die einen aus gesamtgesellschaftlicher Sicht bedeutenden Versorgungsgrad aufweisen mittels Schwellenwerten für jede Anlagenkategorie
   - ❖ Rein quantitatives Verfahren: Schwellenwerte orientieren sich an der Versorgung von 500.000 Menschen
   - ❖ Beispiel: Die Wasserversorgung wird mit einem Jahresdurchschnittsverbrauch von 44 m³ pro Person gerechnet Schwellenwert = 44 m³ * 500.000 = 22 Mio. m³



Was sind letztendlich die To Do`s?

Prävention

- **Angemessene technische / organisatorische Maßnahmen** nach dem *Stand der Technik*
  - Erarbeitung branchenspezifischer Sicherheitsstandards durch die Branchen selbst, BSI stellt auf Antrag Eignung fest
- **Auditierungspflicht**
  - Nachweis alle zwei Jahre durch geeignete Audits, Prüfungen oder Zertifizierung, erstmals 2 Jahre nach Inkrafttreten der BSI-KritisV
- **Meldung von erheblichen Störungen**, die zu Ausfällen oder Beeinträchtigungen der KRITIS führen oder führen können
- **Untersuchung und Empfehlung** von IT-Produkten durch das BSI

Informationssicherheit

Sicherheit der Verarbeitung

- Ziel: Sicherheit der Daten und der Verarbeitung durch technisch-organisatorische Maßnahmen
- Adressaten: Verantwortliche / Auftragsverarbeiter
- Zu berücksichtigende Faktoren:
  - Implementierungskosten, Schwere und Eintrittswahrscheinlichkeit des Risikos für die Rechte der Betroffenen, Verarbeitungsart
- Beispiele: Pseudonymisierung, Verschlüsselung, rasche Wiederherstellung der Verfügbarkeit, Sicherstellung der Vertraulichkeit, regelmäßige Überprüfung („Stand der Technik“)
- Aber: Deutlich höhere Bußgelder (IT-SiG sieht Bußgeld bis zu max. EUR 100.000,00 vor)

Kein europäisches Phänomen

Beispiele

- Konvention über Cybersecurity und den Schutz der persönlichen Daten der Afrikanischen Union

- **Automobilindustrie USA**

  „Security and Privacy in Your Car Act of 2015“
  - Gesetzesentwurf, welcher Datensicherheit (durch Einhalten von Sicherheitsstandards) und Datenschutz (durch Einhalten gewisser Prinzipien bei der Verarbeitung von personenbezogenen Daten) fordert

  „Enhance Automotive Cybersecurity“
  - Eigeninitiative der Automobilindustrie, welche ein Prinzip zur Verbesserung der Sicherheit des öffentlichen Verkehrs enthält

06 > “Dschungel” IT-Sicherheit in Deutschland

Allg. (zivilrechtliche) Haftung / Produkthaftung

DS-GVO

Sondergesetze (TMG / TKG bzw. ePrivacyVO)

IT-SiG / KRITIS

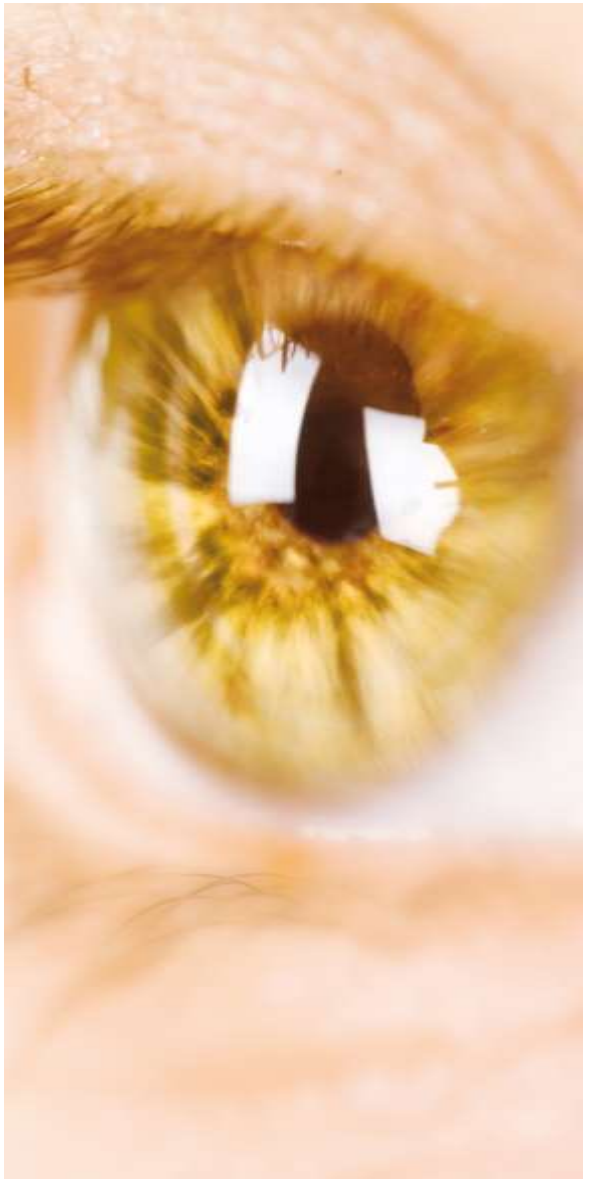
Regulatorische Anforderungen, Internationale Standards

IT-Sicherheits-standards (ISO 27001, BSI Grundschutz etc.)

Was bleibt vom „Kampf“ übrig?

Status Quo und Ausblick

- „Flickenteppich“
- Unterschiedliches Verständnis von gleichen Begriffen innerhalb verschiedener Gesetzen
  - Beispiel: Stand der Technik
- Unklare Anforderungen
  - Entscheidung durch ein Gericht?
  - Wie maßgeblich kann das sein?
- Grundsatzfragen:
  - Reichen die erlassenen Gesetze?
  - Bedarf es mehr Gesetze?
  - Ist ein neuer Ansatz erforderlich?



Wo steht Deutschland?

Lösung – Schnell, effektiv, qualitativ?

- IT-Sicherheit hört nicht an der Grenze auf!
- Agieren, wie in der Wirtschafts- und Flüchtlingskrise
  - Kooperation über die Grenzen hinweg
- Rechtliche Basis für schnelle Abwehr und präventiven Schutz
  - z.B. Vorsehen von Krisenstäben
- Nicht stehen bleiben – Schutz von Mittelstand und Deutschlands „Top-Industrien“
- Bisheriger politischer Aufwand? Gering!

Was ist Ihre Meinung?

TaylorWessing

Ihre Ansprechpartnerin

Ihre Ansprechpartnerin

Mareike Christine Gehrmann
Salary Partnerin, Düsseldorf
Fachanwältin für Informationstechnologierecht

> **Informationstechnologie/Telekommunikation**
> **Datenschutz**
> **Tech-Litigation**

JUVE AWARDS 2015 – Kanzlei des Jahres für Medien und Technologie

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 regelmäßig 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.

Kontaktdaten

T: +49 211 8387-189 E: m.gehrmann@taylorwessing.com

Taylor Wessing im Überblick

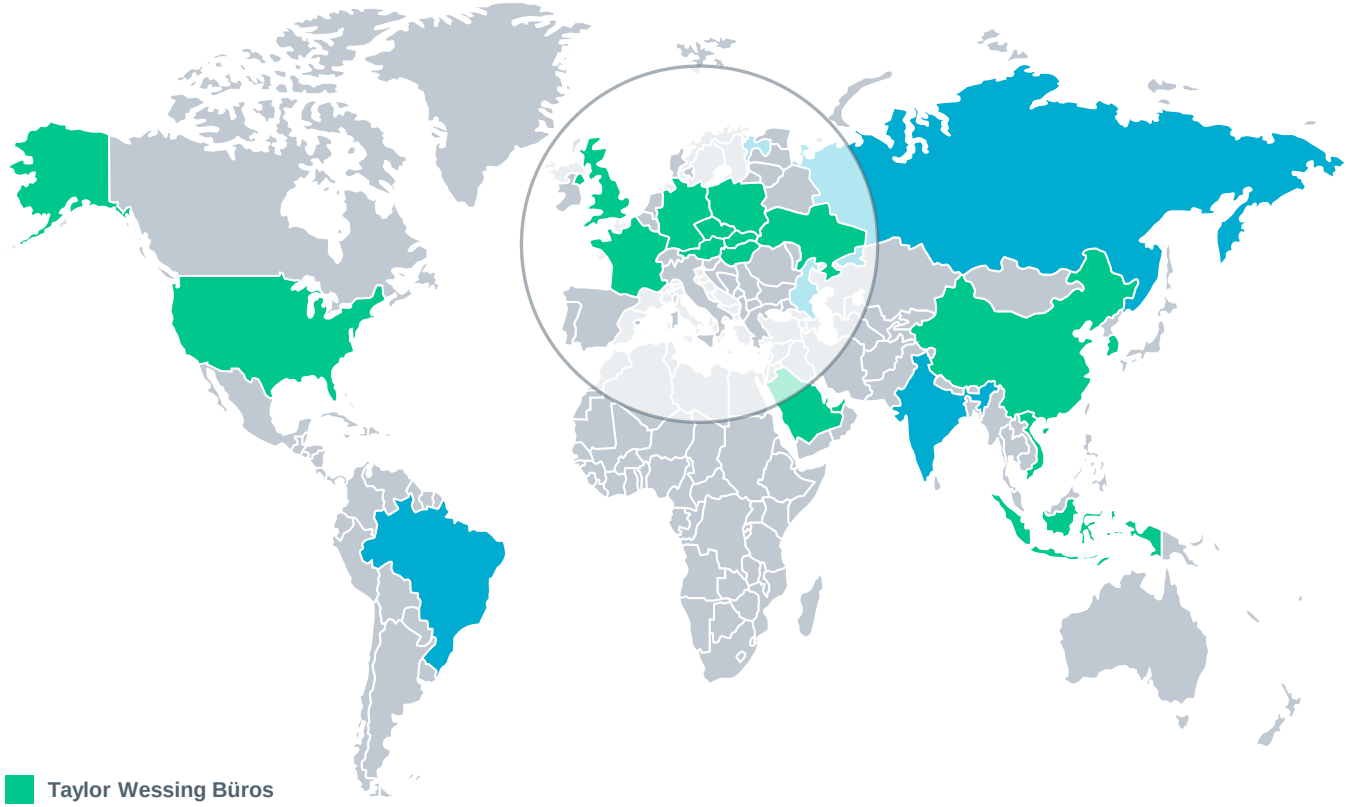
- Führende **internationale Full Service-Kanzlei**
- Praxisnahe Beratung in allen Fragen des **nationalen und internationalen Wirtschaftsrechts**
- **Branchen Know-how** durch langjährige Beratungsbeziehungen zu führenden Unternehmen
- Über **1.200 Rechtsanwälte** an **33 Standorten** in Europa, den USA, dem Mittleren Osten und Asien, einschließlich unserer Kooperationen in Südkorea, Indonesien und Saudi-Arabien
- **Starke Präsenz im asiatischen Raum** durch unsere führende China Praxis mit Repräsentanzen in Beijing, Shanghai und Hongkong sowie Büros in Singapur, Seoul und Jakarta
- **Expertenteams** für die Wirtschaftsregionen Brasilien, Russland und Indien
- **Internationales Netzwerk** von ausgewählten und erprobten Kooperationskanzleien in weiteren Ländern

JUVE AWARDS 2016 · FIRM OF THE YEAR 2016 · THE TRANSATLANTIC LEGAL AWARDS WINNER 2016 · JUVE AWARDS 2015 · IP FIRM OF THE YEAR 2012 · THE LAWYER AWARDS 2013 TRAVELERS WINNER · JUVE AWARDS 2010

TaylorWessing

Standorte und Netzwerk

Wir verfügen über ein ausgewähltes Netzwerk von Partnerkanzleien, mit denen wir seit vielen Jahren bei grenzüberschreitenden Transaktionen und Projekten in allen wichtigen Rechtsgebieten zusammenarbeiten.



Taylor Wessing Büros

Taylor Wessing Expertenteams und Ländergruppen

Kooperationskanzleien über internationales Netzwerk

Belgien
Brüssel

China
Peking* I Shanghai*

Deutschland
Berlin I Düsseldorf I
Frankfurt I Hamburg I München

Frankreich
Paris

Großbritannien
Cambridge I London

Hongkong

Indonesien
Jakarta**

Niederlande
Amsterdam | Eindhoven

Österreich
Klagenfurt* I Wien

Polen
Warschau

Saudi-Arabien
Dschidda** I Riad**

Singapur

Slowakei
Bratislava

Südkorea
Seoul**

Tschechische Republik
Brünn* I Prag

Ungarn
Budapest

Ukraine
Kiew

USA
Silicon Valley* I New York*

Vereinigte Arabische Emirate
Dubai

Vietnam
Hanoi I Ho-Chi-Minh-Stadt

* Repräsentanzen ** Assoziierte Büros

TaylorWessing

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 **Münchner 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. Erstmalig werden auch Industrieaspekte miteinbezogen. Die fünfte Auflage wird in Kürze veröffentlicht.

Unsere IoT-Expertise:
https://deutschland.taylorwessing.com/de/internet-of-things

TaylorWessing