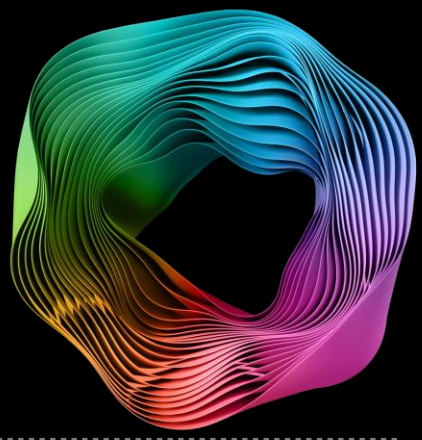
Deloitte. Legal



Cybersicherheit & Recht

Zeitalter digitaler Bedrohungen

Cyberangriffe, Datenschutzverletzungen und Ausfälle kritischer Infrastruktur zählen zu den gravierendsten unternehmerischen Risiken unserer Zeit. Mit der EU-Cyberregulierung und der wachsenden nationalen Regulierung entsteht ein komplexes, sich rasch veränderndes Regulierungsumfeld. Unternehmen sind gezwungen, technische Sicherheitsmaßnahmen mit rechtlichen Compliance-Anforderungen in Einklang zu bringen – und das in einer Zeit, in der die Bedrohungslandschaft immer komplexer wird und exponentiell wächst. Wer nicht proaktiv handelt, riskiert empfindliche Bußgelder, Haftungsansprüche und Reputationsverluste.

Rechtsrahmen und Handlungsfelder

Die Regulierung der Cybersicherheit ist vielschichtig und umfasst europäisches sowie nationales Recht. Zu den zentralen Regelwerken zählen die **NIS2-Richtlinie** (Netz- und Informationssicherheit), der **EU Cyber Resilience Act (CRA)**, die **DORA-Verordnung** (digitale operationale Resilienz für den Finanzsektor), das **IT-Sicherheitsgesetz 2.0**, die **DSGVO** sowie branchenspezifische Anforderungen aus dem Energie-, Gesundheits- und Finanzsektor.

Daraus ergeben sich insbesondere folgende Handlungsfelder:

- **Cyber Compliance** – Umsetzung gesetzlicher Cybersicherheitspflichten
- **Incident Response** – Rechtssichere Reaktion auf Sicherheitsvorfälle
- **Lieferkettensicherheit** – Vertragsgestaltung und Haftungsfragen
- **KRITIS-Regulierung** – Betreiberpflichten für kritische Infrastrukturen
- **Datenschutz & Cybersicherheit** – Identifikation von Schnittstellen und Konfliktfeldern

Rechtliche, operative und strategische Herausforderung

Die rechtliche Bewältigung von Cybersicherheitsrisiken bewegt sich in einem Spannungsfeld: **Regulatorische Konformität** versus **operative Flexibilität**, **Meldepflichten** versus **strategische Kommunikation**, **Drittanbieterabhängigkeit** versus **eigenverantwortliche Compliance**. Hinzu kommen Haftungsfragen bei Sicherheitsvorfällen, Anforderungen an die Protokollierung und Nachweisführung sowie die rechtssichere Einbindung von Cloud-Diensten und KI-gestützten Sicherheitssystemen. Insbesondere die grenzüberschreitende Natur von Cyberbedrohungen macht eine ganzheitliche, interdisziplinäre Betrachtung unumgänglich.

Warum jetzt agieren? **Wer frühzeitig in eine rechtskonforme Cybersicherheitsstrategie investiert, reduziert Haftungsrisiken, vermeidet Bußgelder und schützt seinen Ruf als verlässlicher und vertrauenswürdiger Marktteilnehmer – gegenüber Kunden, Partnern und Behörden gleichermaßen.**

HANDLUNGSFELDER

Unternehmen, die IT-Infrastrukturen betreiben, digitale Produkte entwickeln oder kritische Dienste erbringen, stehen vor der Herausforderung, technische Sicherheitsanforderungen mit einem immer dichter werdenden Regulierungsrahmen zu verbinden. Eine frühzeitige rechtliche Auseinandersetzung mit Cybericherheitspflichten und die Identifizierung von relevanten Maßnahmen ist dabei entscheidend.

Aufgaben

- ✓ **NIS2-Readiness Assessment** – Analyse der Betroffenheit, Bewertung der Meldepflichten und Umsetzungsplanung gemäß NIS2-Richtlinie und nationalem Umsetzungsgesetz
- ✓ **Cyber Resilience Act (CRA) Compliance – Sicherstellung der Produktanforderungen für** Hersteller vernetzter Geräte und Software über den gesamten Lebenszyklus
- ✓ **DORA-Compliance** – Erfüllung operationaler Resilienzanforderungen, IKT-Risikomanagement und Meldepflichten
- ✓ **Incident Response & Krisenmanagement** – Planung und Management von Cyberangriffen, einschließlich Behördenkommunikation und Haftungsminimierung
- ✓ **Vertragsgestaltung & Lieferkettensicherheit** – Ausgestaltung von IT-Dienstleistungs- und Lieferantenverträgen unter Berücksichtigung gesetzlicher Cybersicherheitspflichten
- ✓ **Training & Befähigung** – Schulung von Führungskräften, Compliance- und IT-Teams zu rechtlichen Cybersicherheitspflichten und deren praktischer Umsetzung

Unsere Services

Deloitte Legal & Deloitte: As One Deloitte beraten wir umfassend zum Thema Cybersicherheit und Recht.

- ✓ **Ganzheitliche rechtliche und regulatorische Beratung entlang der gesamten Cybersicherheits-Compliance-Kette – von der Risikoanalyse bis zur behördlichen Kommunikation**
- ✓ **Ausbau und Überprüfung von Cyber-Governance-Strukturen sowie rechtlicher Rahmenbedingungen für das IT-Risikomanagement**
- ✓ **Prüfung und Gestaltung sämtlicher rechtlicher Beziehungen mit Blick auf Cybersicherheit – von der Lieferkette über Cloud-Verträge bis zu Versicherungslösungen**

IHR KONTAKT

Dr. Söntje Julia Hilberg, LL.M.

Rechtsanwältin I Partner
Co-Lead Digital Law
E-Mail: shilberg@deloitte.de
Phone: +49 30 254683016
Mobile: +49 170 7663353

Juliane Franze

Rechtsanwältin I Senior Manager
E-Mail: jfranze@deloitte.de
Phone: +49 30 254683656
Mobile: +49 151 54484834