

TaylorWessing

Cybersicherheitsrecht 2.0

Was bringen NIS-2, DORA & CRA für Unternehmen

08. November 2024

Thomas Kahl

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance		
Digital Europe Programme Regulation, (EU 2021/694)	Recovery and Resilience Facility Regulation, (EU 2021/241)	Frequency Bands Directive, (EEC) 1987/2172	European Statistics, (EC) 2006/223, 2023/0023(COD)	Database Directive, (EC) 1996/95	Regulation for a Cybersecurity Act, (EU 2019/891), 2023/0096(COD)	Law Enforcement Directive, (EU 2016/680)	Product Liability Directive (PLD), (EC) 1985/274, 2022/0300(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/39, update 3005	Satellite and Cable I Directive, (EEC) 1993/63	Common VAT system, (EC) 2006/112, 2022/0467(COD)		
Horizon Europe Regulation, (EU 2021/696), (EU 2021/794)	Erasmus+ Programme Regulation, (EU 2021/693)	Radio Spectrum Decision, (EC) 2002/976	General Data Protection Regulation (GDPR), (EU 2016/679)	Community Design Directive, (EC) 2001/8, 2022/0281(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU 2021/687)	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU 2014/723)	Toys Regulation, (EC) 2009/48, 2023/0230(COD)	Price Indication Directive, (EC) 1998/6	Technology Transfer Block Exemption, (EC) 2014/918	Information Society Directive, (EC) 2000/39	Administrative cooperation in the field of taxation, (EU 2011/16)		
Regulation on a pilot regime distributed ledger tech. markets, (EU 2021/688)	Connecting Europe Facility Regulation, (EU 2021/1152)	Broadcast Cost Reduction Directive, (EU 2014/61), 2023/0056(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU 2018/772)	Enforcement Directive (IPR), (EC) 2004/48	MIS 2 Directive, (EU 2022/2555)	Regulation on interoperability between EU information systems in the field of borders and visa, (EU 2018/917)	European Standardisation Regulation, (EU 2019/1025)	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU 2017/133, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU 2010/13)	Payment Service Directive 2 (PSD2), (EU 2015/2366, 2023/0028(COD)		
	Regulation on High Performance Computing Joint Undertaking, (EU 2021/1172)	Open Internet Access Regulation, (EU 2015/2120)	Regulation on the free flow of non-personal data, (EU 2018/1807)	Directive on the protection of trade secrets, (EU 2016/942)	Information Security Regulation, 2022/0064(COD)	Regulation on terrorist content online, (EU 2021/784)	eIDAS Regulation, (EU 2014/513), 2023/0138(COD)	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU 2019/1020)	Portability Regulation, (EU 2017/1128)	Digital Operational Resilience Act (DORA) Regulation, (EU 2022/2554)		
	Regulation on Joint Undertakings under Horizon Europe, (EU 2021/098, 2022/0033(COD)	European Electronic Communications Code Directive (EECC), (EU 2018/1972)	Open Data Directive (PSI), (EU 2019/1024)	Design Directive, 2022/0022(COD)	Cybersecurity Regulation, 2022/0089(COD)	Temporary CSAM Regulation, (EU 2021/733, 2022/0166(COD)	Radio Equipment Directive (RED), (EU 2014/53, 2022/0143(COD)	Directive on Consumer Rights (CRD), (EU 2011/63, 2022/0114(COD)	FSE Regulation, (EU 2019/1149)	Satellite and Cable II Directive, (EU 2014/538)	Crypto-assets Regulation (MCA), (EU 2023/0114)		
	Decision on a path to the Digital Decade, (EU 2022/048)	au top-level domain Regulation, (EU 2018/657)	Data Governance Act (DGA Regulation), (EU 2023/096)	Compulsatory licensing of patents, 2022/0128(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU 2022/3542)	Regulation for a Single Digital Gateway, (EU 2018/1724)	e-invoicing Directive, (EU 2012/65)	Single Market Programme, (EU 2014/609)	Copyright Directive, (EU 2019/793)	Financial Data Access Regulation, 2022/0205 (COD)		
	European Chips Act (Regulation), (EU 2022/1781)	Roaming Regulation, (EU 2022/672)	ePrivacy Regulation, 2012/0003(COD)	Standard essential patents, 2022/0133(COD)	Cyber Solidarity Act (Regulation), 2022/0109(COD)	Directive on combating violence against women, 2022/0066(COD)	General Product Safety Regulation, (EU 2019/1998)	Geo-Blocking Regulation, (EU 2015/2302)	Vertical Block Exemption Regulation (VBEE), (EU 2022/2720)	European Media Freedom Act, 2022/0217(COD)	Payment Services Regulation, 2009/0210(COD)		
	European critical raw materials act (Regulation), 2022/0078(COD)	Regulation on the Union Secure Connectivity Programme, (EU 2023/058)	European Data Act (Regulation), 2023/0043(COD)			Digitalisation of travel documents	Machinery Regulation, (EU 2017/1220)	Regulation on cooperation for the enforcement of consumer protection laws, (EU 2017/2294)	Digital Market Act (DMA Regulation), (EU 2022/1925)	Renunciation of royalties from third countries for recorded music played in the EU	Digital euro, 2022/0117 (COD)		
	Net Zero Industry Act, 2022/0001(COD)	New radio spectrum policy programme (RSPP 3.0)	European Health Data Space (Regulation), 2022/0149(COD)				AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU 2019/770)	Regulation on distortive foreign subsidies, (EU 2022/2580)		Regulation on combating late payment, 2002/0020(COD)		
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0118(COD)	Digital Networks Act	Regulation on data collection for short-term rental, 2022/0258(COD)				Eco-design Regulation, 2022/0005(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU 2019/771)	Horizontal Block Exemption Regulations (H-BER), (EU 2022/0166, (EU 2022/1967)				
	EU Space Law		Interoperable Europe Act, 2022/0027(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU 2022/2066)	Platform Work Directive, 2021/0318(COD)				
	Initiative to open up European supercomputer capacity to startups		Harmonization of GDPR enforcement, 2022/0220(COD)					Political Advertising Regulation, 2021/0381(COD)	Single Market Emergency Instrument (SMRE), 2022/0278(COD)				
			Access to vehicle data, functions and resources					Right to repair Directive, 2022/0906(COD)					
Green Data Act			Multimodal digital mobility services (MDMS)										
								Consumer protection strengthened enforcement cooperation					

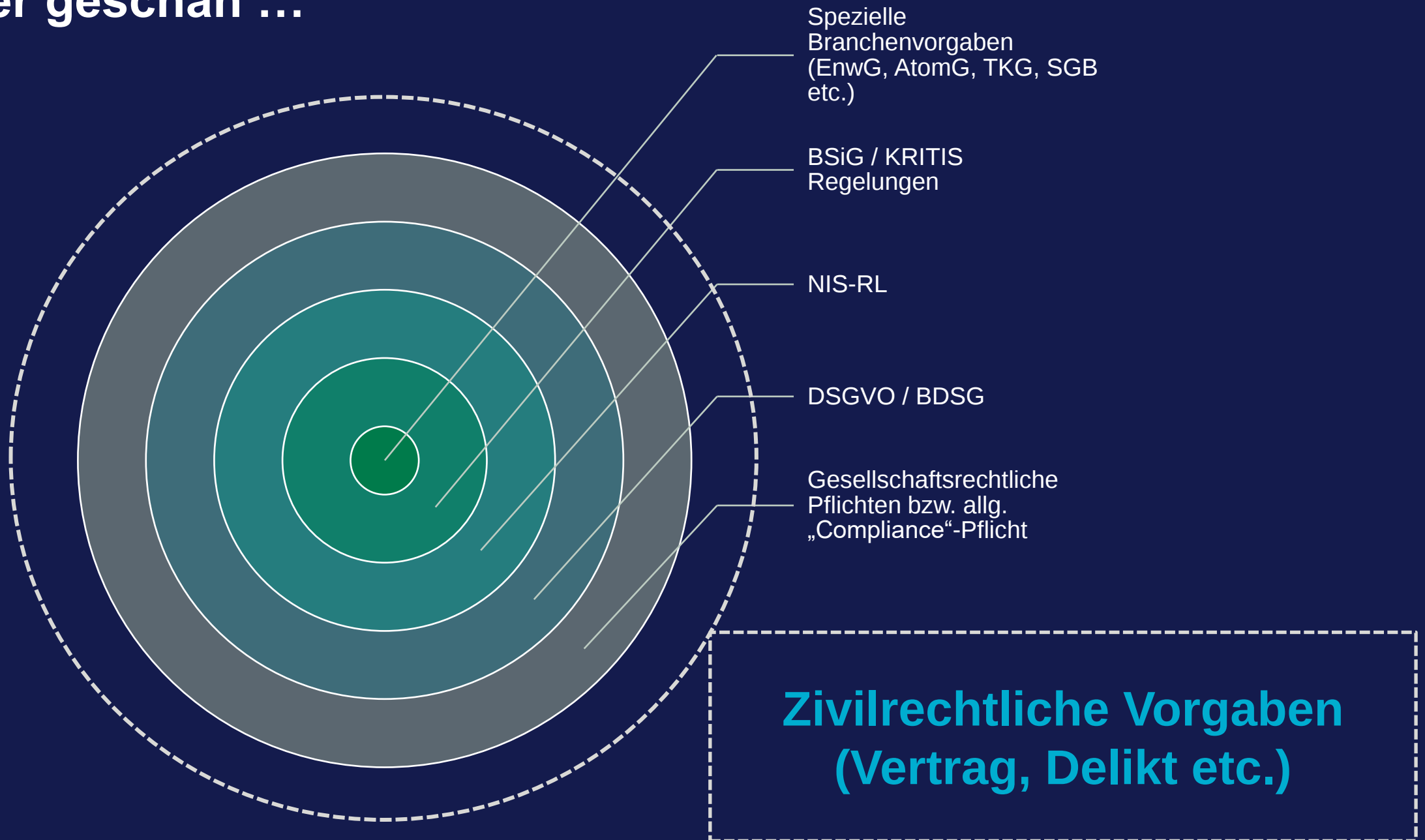
Quelle: https://www.bruegel.org/sites/default/files/2023-11/Bruegel_factsheet.pdf

Aktuelle Digital-Gesetzgebung der EU – ein Flickenteppich!



Applicable law	Published in the Official Journal of the European Union
In negotiation	Proposal by the European Commission entered the legislative process.
Planned initiative	Mentioned by the European Commission as potential legislative initiative

Was bisher geschah ...



Warum so viele neue Regelungen?



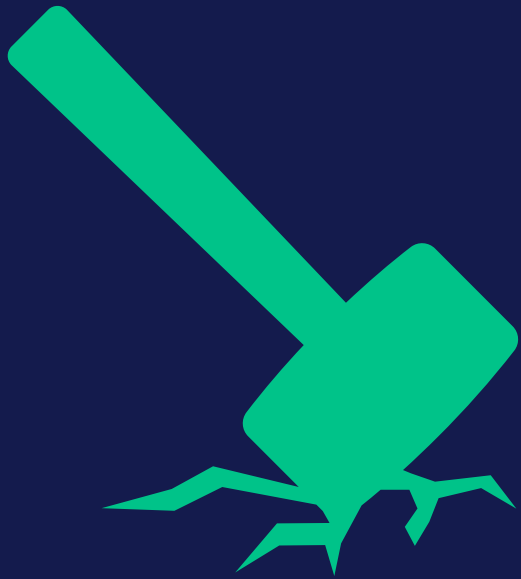
- 1 Flickenteppich an Rechtsvorschriften in unterschiedlichsten Bereichen
- 2 Gedanke des präventiven Schutzes der IT-Infrastruktur (Cybersicherheitsattacken + systemische Non-Compliance)
- 3 Im Interesse der Allgemeinheit

Was wir nun beobachten ...



- 1 Erhebliche Ausweitung der IT-Sicherheitsgesetzgebung auf Unternehmen / Branchen, die zuvor nur von “allgemeinen” Vorgaben betroffen waren
- 2 IT-Sicherheitsgesetzgebung mit einem zusehends starken Fokus auf “Governance”
- 3 IT Sicherheit wird zum Gewährleistungs- und Haftungs-Thema, wobei sich die Pflichten insbesondere in zeitlicher Hinsicht erheblich ausweiten (“Lifecycle”)

Das ist für Unternehmen schwierig, weil ...



- 1** Viele Unternehmen nicht darauf vorbereitet sind (Stichwort “Governance” und “Supply Chain”)
- 2** Die Regelungen teils vollkommen unklar sind (Stichwort “Konzern-Privileg”)
- 3** Die Gesetze teils schwierige Wechselwirkungen untereinander und mit anderen Regelwerken erzeugen

Was haben wir vor?



- 1 2. EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2)
- 2 Digital Operational Resilience Act (DORA)
- 3 Cyber Resilience Act (CRA)

1 | NIS-2

NIS-2 im Überblick



- Umsetzungsfrist abgelaufen
- Umsetzung durch NIS-2 Umsetzungsgesetz-E im BSiG
- Inkrafttreten avisiert für Q1 / Q2 2025



- Wichtige vs. besonders wichtige „Einrichtungen“ vs. KRITIS-Betreiber (gelten als besonders wichtig)
- Erhebliche Absenkung der Schwellenwerte
- Erhebliche Ausweitung der Sektoren (u.a. IT-Services)
- > 25.000 neue Unternehmen betroffen

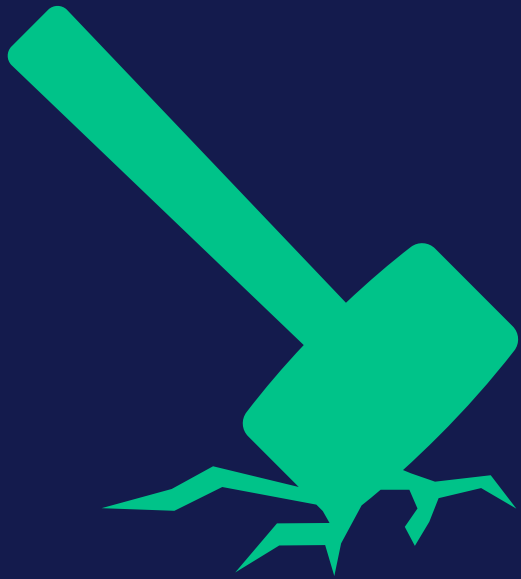


- Erweiterte Pflichten für wichtige Einrichtungen (v.a. Präventionsmaßnahmen, Einbeziehung von Lieferketten)
- Erweiterte Governance-Pflichten und Haftung
- Dreistufiges Melderegime
- Verschärfte Aufsichts- und Durchsetzungsbefugnisse



- Bis zu 10 / 7 Mio. EUR; wenn Umsatz mehr als 500 Mio. EUR bis zu 1,4 / 2 % des weltweiten Jahresumsatzes
- Prüfung (je nach Kategorie auch anlasslos), Anweisung, Untersagung

Warum hat das so einen Impact?



- 1** Anforderungen an “Governance” und “Supply Chain” stellen Unternehmen vor große praktische Herausforderungen
- 2** Regelungen sind teils vollkommen unklar (Schwellenwert-Berechnung, betroffene Systeme / Teile der Einrichtung, Konzernsachverhalte, “Cloud“-Fälle)
- 3** Umsetzung der Meldepflichten (24 Std.) und Organisation im Unternehmen in Abstimmung mit anderen Stellen / Abteilungen / Konzern

2 | DORA

DORA im Überblick



- Inkrafttreten in 2023
- Gilt vollständig ab Januar 2025



- Sonderregelungen für Unternehmen der Finanzindustrie wie Kreditinstitute, Handelsplätze und Versicherungen sowie IKT-Drittdienstleister in allen EU-Mitgliedsstaaten
- Lex specialis zu NIS-2 (vgl. Erwägungsgrund 28 NIS 2 und Art. 4 Abs. 1 NIS 2) für Finanzunternehmen
- „Doppelregulierung“ für IKT-Dienstleister

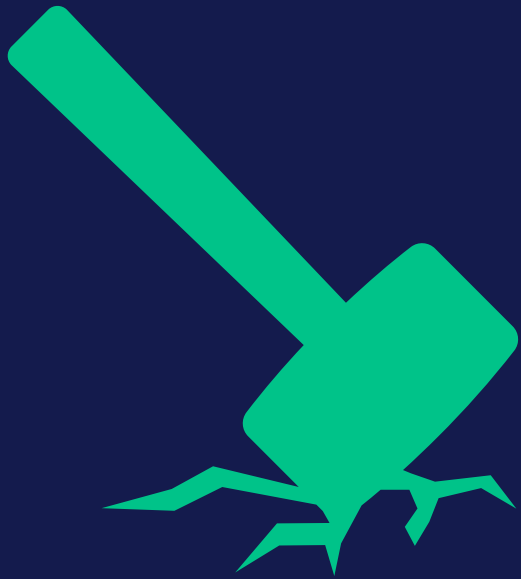


- Umfangreiche Pflichten wie Risikomanagement, Incident Management, Stresstests, IKT-Drittpartei-Risk (konkretisiert durch RTS)
- Umfassende Vorgaben für IKT-Risk Management (Konzentration, Audit, Register) und Vertragsmanagement (Kündigung, Exit-Strategie, Schulung)
- „Kritische“ IT-Provider mit eigenen umfangreichen Pflichten und eigener EU-Aufsicht
- DORA-Pflichten lassen sich teilweise NIS2 zuordnen



- Aufsicht durch ESA (versch. Behörden)
- Prüfung, Anweisung, Untersagung
- Sanktionsbefugnisse

Warum hat das so einen Impact?



- 1** Praktische Herausforderungen der 3rd Party IKT Risiko-Vorgaben für Finanzunternehmen und Rollout im (Supplier-)Netzwerk
- 2** Wechselwirkungen mit NIS-2 (u.a. für IKT-Provider)
- 3** Erhebliche Beschränkung der Vertragsgestaltung für IKT-Provider (Kündigung, Transition, SLAs etc.)

3 | CRA

CRA im Überblick



- Verabschiedet - Inkrafttreten noch in 2024
- Mai 2026: KBS können Bewertung vornehmen
- Aug 2026: Meldepflicht für Schwachstellen und Sicherheitsvorfälle
- Nov 2027: Vollständige Geltung



- Erweiterte Cybersicherheitsvorgaben für vernetzte Produkte mit „digitalen Elementen“ in der EU
- Für Hersteller, Importeure und Distributoren
- Gilt nicht für anderweitig regulierte Produkte (z.B. Automotive, Medizinprodukte, zivile Luftfahrt)



- Standard / wichtig / kritisch (u.a. PW Manager, Firewalls, Smartcards, intelligente Zähler)
- Security by design & default
- Dokumentation durch Software Bill of Materials (SBOM)
- Konformitätserklärung (teils mit 3rd Party Assessment)
- Product-Lifecycle
- Meldepflichten



- Geldbußen bis zu 15 Mio EUR or 2,5 % des weltweiten Jahresumsatzes
- Verbot / Beschränkung des Vetriebs des Produkts / Rückruf
- Ansprüche von Kunden, Wettbewerbern, Interessengruppen

Who is who in CRA?

Manufacturer

Anforderungen

- Security by design („Essential Requirements“, Annex I)
- Risk Assessment & Dokumentation
- Report Vulnerabilities (24/72)
- Monitoring & Updates während „Support Period“ (Minimum 5 J. - 10 J.)
- Conformity Assessment / Declaration & CE Marking (für „important“ and „critical“ Provider via 3rd Party Assessment)

Importer

Prüfpflichten

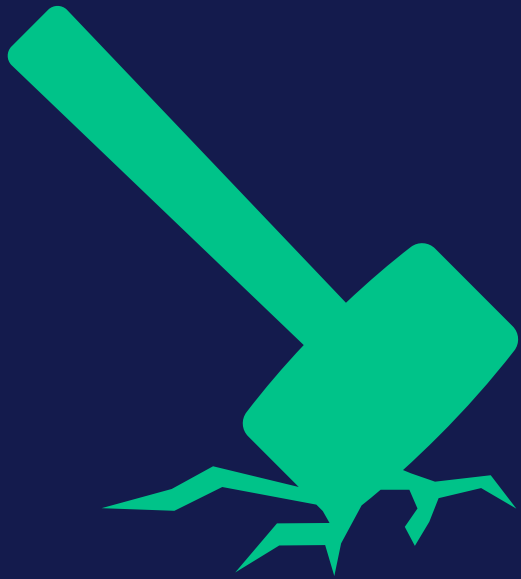
- ✓ Conformity Assessment Procedure korrekt beim Hersteller?
- ✓ Technical Documentation & CE Marking ok?
- ✓ Transparency-Check (Nutzungsanleitung)
- ✓ Einhaltung der “Essential Requirements” (Annex I)

Distributor

Prüfpflichten

- ✓ CE Marking ok?
- ✓ Information / Instructions / EU Declaration of Conformity ok?
- ✓ Importer Name / Trade Name / Trademark und Kontaktadresse auf der Produktverpackung?

Warum hat das so einen Impact?



- 1** Erweiterung der Produktsicherheits- und Konformitätsvorgaben um IT-Sicherheit (Gewährleistung / Haftung)
- 2** Vorgaben des Lifecycle-Managements greift erheblich in kommerzielle Kalkulation / Business-Prozesse ein
- 3** Wechselwirkung mit Produkt-Regulierung und schwierige Abgrenzungsfragen

IHRE FRAGEN

Ihr Ansprechpartner

Thomas Kahl ist Fachanwalt für Informationstechnologierecht. Er berät nationale und internationale Unternehmen in allen rechtlichen Fragen rund um Informationstechnologien. Mit seiner Expertise begleitet er Digitalisierungsprojekte und die Implementierung innovativer Technologien. Er ist Experte für die Umsetzung der Anforderungen der DSGVO sowie branchenspezifischer Anforderungen des Daten- und Datenschutzrechts mit Schwerpunkt in den Bereichen Automotive & Mobility und regulierte Branchen.

Er leitet die Industry Group Automotive & Mobility der Sozietät.

Thomas Kahl verfügt über umfangreiche Erfahrung in der Beratung von Automobilherstellern in den Bereichen Daten-, Datenschutz-, IT- und IT-Sicherheitsrecht. Er berät Unternehmen regelmäßig bei Datenschutzvorfällen, Cyberangriffen und (datenschutzrechtlichen) Auseinandersetzungen und behördlichen Verfahren.

Thomas Kahl ist in vielen branchenspezifischen Arbeitsgruppen und Verbänden aktiv. Er ist Mitglied der DGRI, aktiv in BITKOM und BVDW sowie Mit-Gründer des iapp-Rhein-Main-Chapters. Er hält regelmäßig Seminare und Vorträge, unter anderem beim BvD e.V. sowie der Beck Akademie, und gibt sein Wissen als Dozent an der Frankfurt School im Rahmen des Certified Compliance Professional (CCP)-Kurses weiter.

Languages: German, English

Find more on Thomas
@ taylorwessing.com



Recommended lawyer for IT and data protection - [Legal 500 2022-24](#)

Tier 1 Law Firm for Data Protection - [Legal 500 Germany 2017-2024](#)

Awarded 5 Stars in the Category Data Protection - [JUVE 2021-2024](#)

Law Firm of the Year for Data Protection, [Handelsblatt 2024](#)



Thomas Kahl

**Partner
Frankfurt**

+49 69 97130-111
t.kahl@taylorwessing.com

Key Areas

- Data Protection & Cyber
- Information Technology
- Litigation & Dispute Resolution



