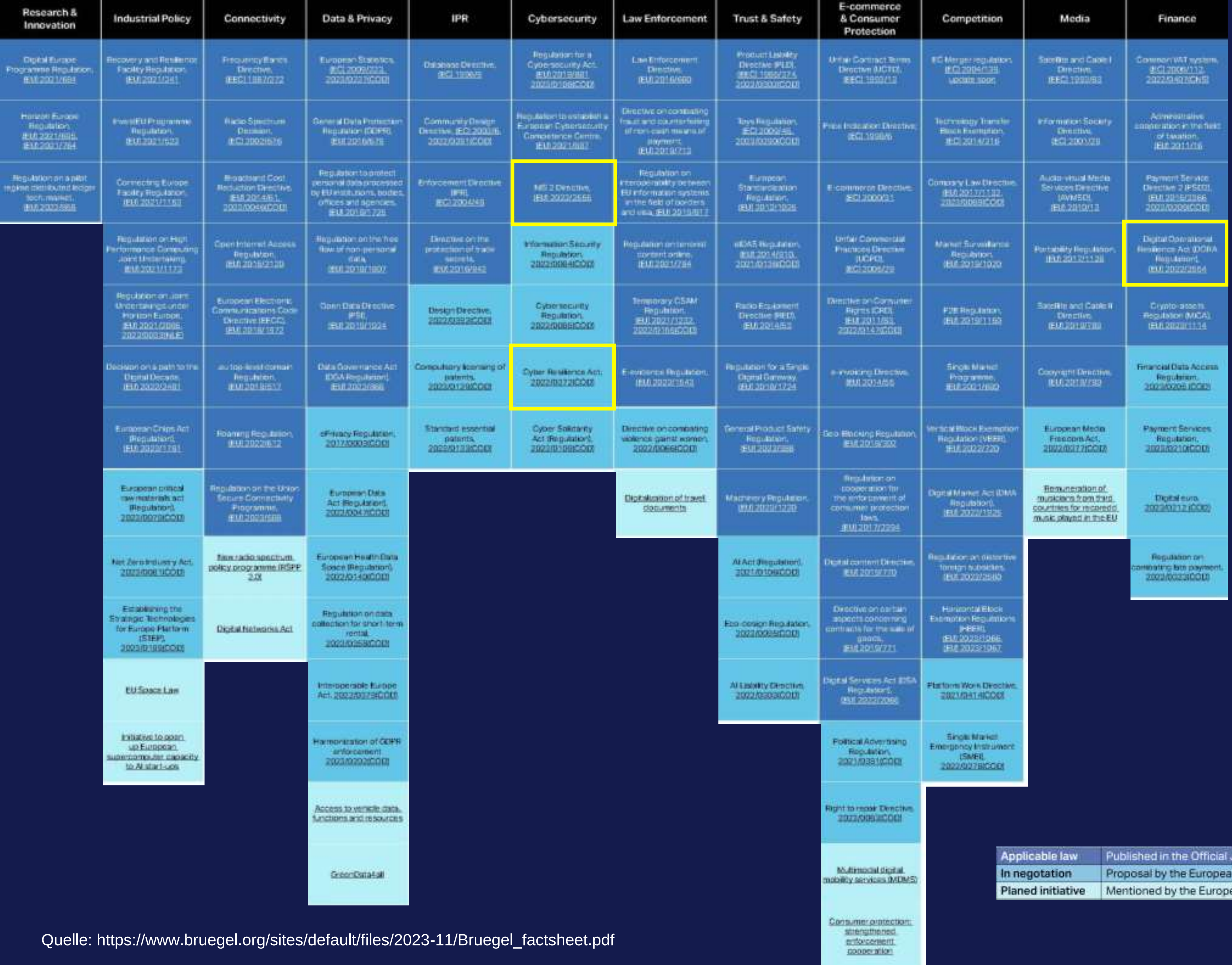
TaylorWessing

Cybersicherheitsrecht 2.0
Was bringen NIS-2, DORA & CRA für Unternehmen

08. November 2024

Thomas Kahl

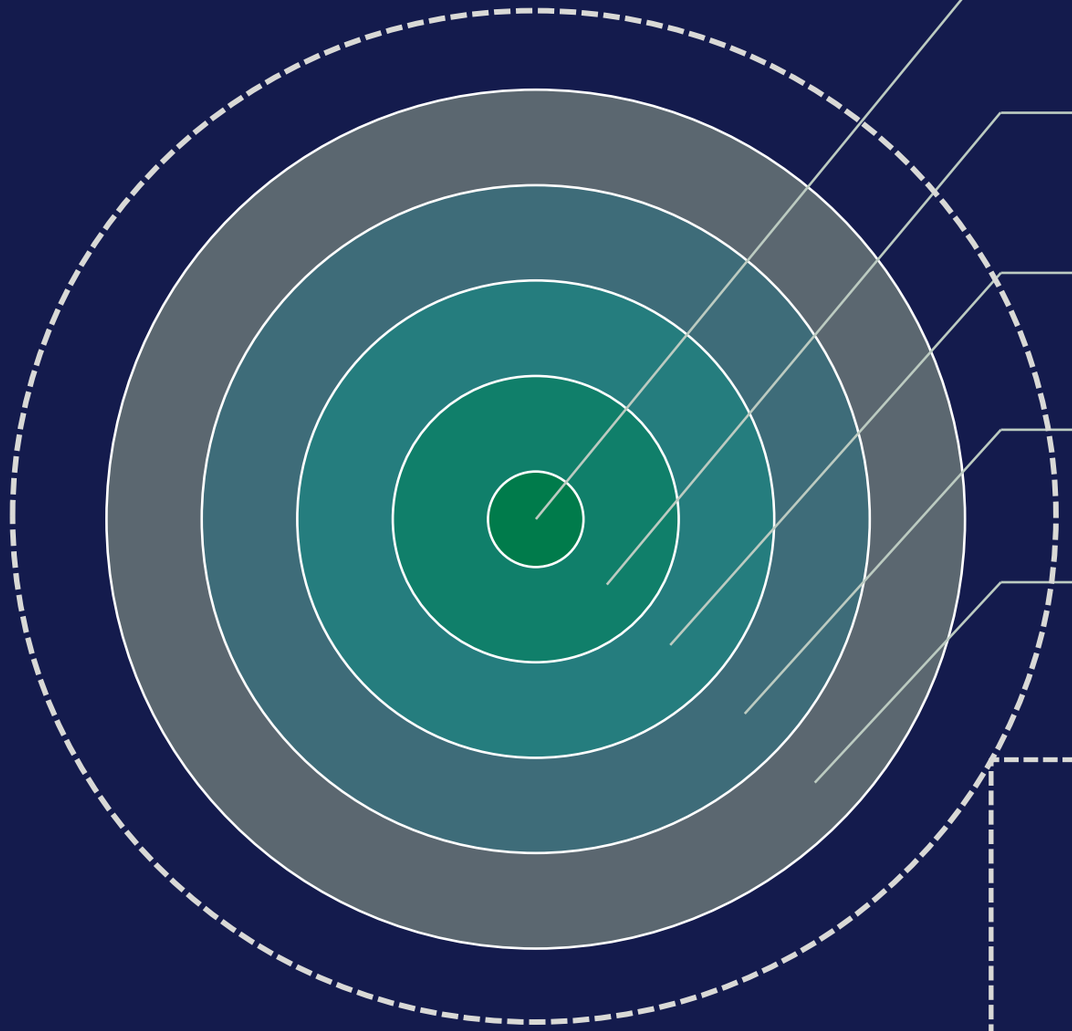


Aktuelle Digital-Gesetzgebung der EU – ein Flickenteppich!

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

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

Was bisher geschah …



Spezielle Branchenvorgaben (EnwG, AtomG, TKG, SGB etc.)

BSiG / KRITIS Regelungen

NIS-RL

DSGVO / BDSG

Gesellschaftsrechtliche Pflichten bzw. allg. „Compliance“-Pflicht

Zivilrechtliche Vorgaben (Vertrag, Delikt etc.)

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

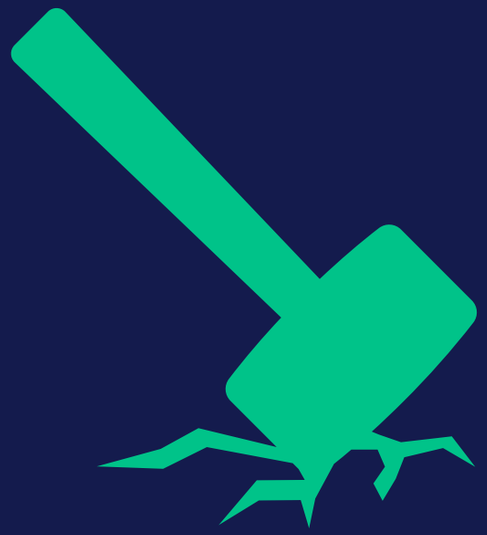
Was wir nun beobachten …

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

TaylorWessing

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

TaylorWessing

DORA im Überblick

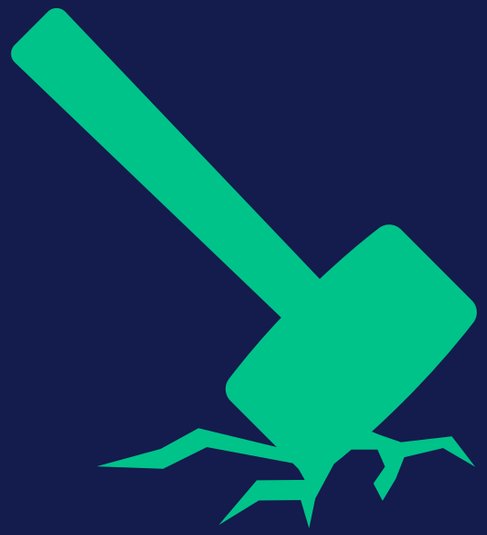
- Inkrafttreten in 2023
- Gilt vollständig ab Januar 2025

- 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

TaylorWessing

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 Cybersicherheits-vorgaben für vernetze 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 Kontaktaddresse 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 Abgrenzungfragen

IHRE FRAGEN

TaylorWessing

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) Auseinandersetzung 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

"

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

Find more on Thomas
@ taylorwessing.com

Thomas Kahl

Partner
Frankfurt

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

Key Areas

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

Europe > Middle East > Asia

taylorwessing.com