NIS2 & KI-Verordnung kompakt: Ein Überblick für Anbieter von Sicherheitslösungen

Wer bin ich?

Diane R. Frank

Fachanwältin für IT-Recht | Partnerin bei Schmid Frank Rechtsanwälte

- Gründungspartnerin der auf IT-Recht & Compliance spezialisierten Kanzlei **Schmid Frank Rechtsanwälte**, Augsburg
  → 9-köpfiges Team: Fachanwälte, Datenschutzbeauftragte, Auditor:innen, Coaches, Ombudsstelle
- **Langjährige Inhouse-Erfahrung** als Justiziarin in großen internationalen IT-Unternehmen
  → Tätigkeit u. a. als **Contract Negotiator** & Vertragsjuristin für komplexe IT-Projekte
- **Seit über 20 Jahren** Beraterin im IT- und Datenschutzrecht
  → Spezialisiert auf **Compliance-as-a-Service**, regulatorische Umsetzung & IT-Vertragsrecht
- **Dozentin & Autorin** im Bereich Datenschutz und Compliance (seit 2012)
- **Zertifizierte Datenschutzbeauftragte & Datenschutzauditorin**
- **International tätig**, Beratung in **7 Sprachen**

EU-Regulierungen zur Cybersicherheit

NIS2-Richtlinie und nationale Regelung

Umsetzung in nationales Recht erforderlich

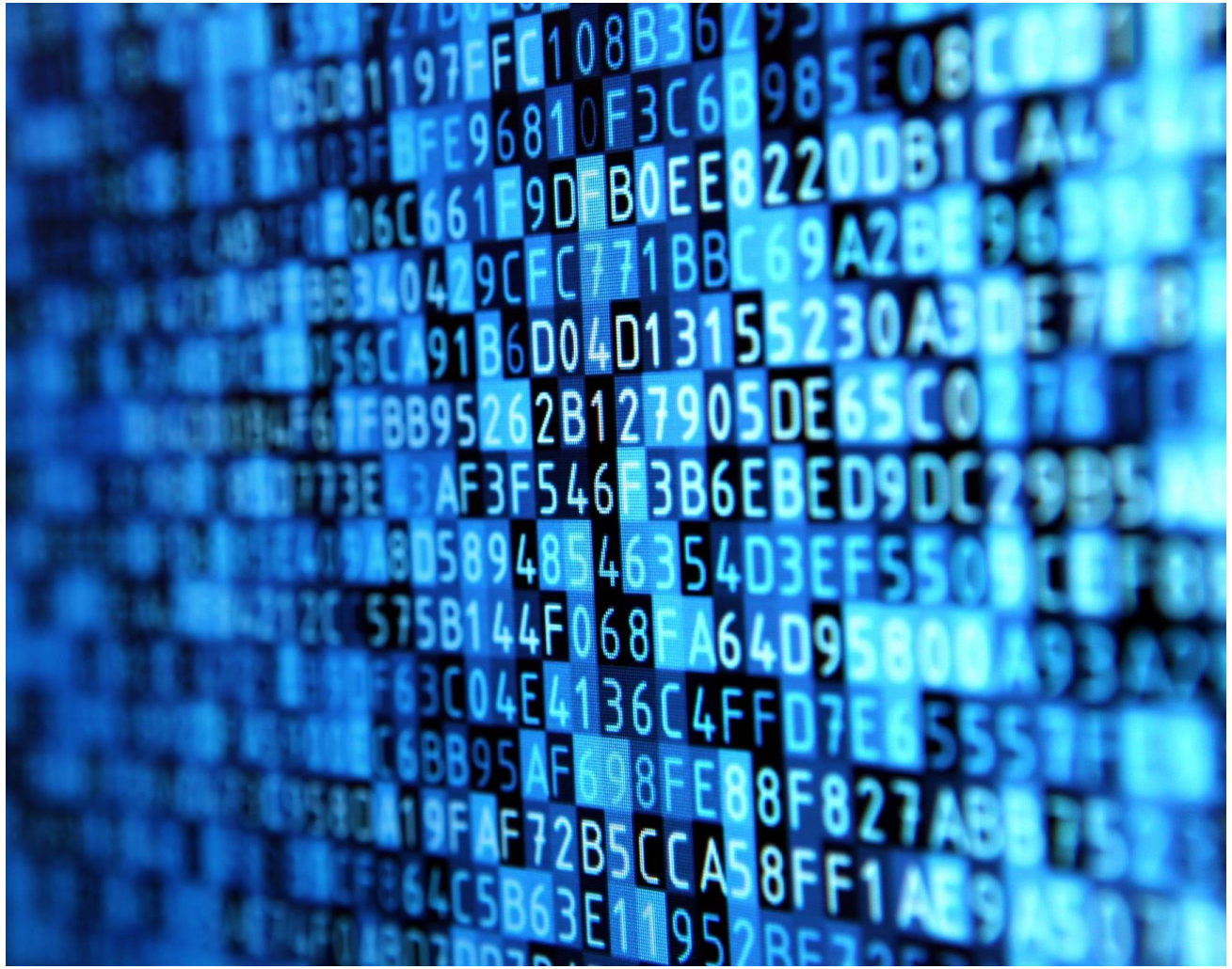
Ziel

Stärkung der Cybersicherheit in der EU

•Verbesserung der Resilienz & Reaktionsfähigkeit von Organisationen in kritischen Sektoren

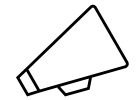
•Gilt für öffentliche und private Einrichtungen in Bereichen wie:

- Telekommunikation & IKT
- Digitale Dienste
- Energie, Verkehr & Gesundheit
- Wasser- & Abfallwirtschaft
- Raumfahrt & Herstellung kritischer Produkte
- Post- & Kurierdienste
- Öffentliche Verwaltung



Zentrale Anforderungen

- Risikomanagement & Notfallplanung
  - Einführung technischer und organisatorischer Maßnahmen
  - Business Continuity Management (BCM)
- Meldepflichten bei Sicherheitsvorfällen
  - Schnelle und strukturierte Informationsweitergabe an Behörden
- Registrierung & Transparenz
  - Verpflichtende Registrierung betroffener Einrichtungen
  - Regelmäßige Berichterstattung
- Informationspflichten
  - Interne und externe Kommunikation bei Vorfällen & Risiken
- Pflichten für Geschäftsleitungen
  - Verantwortung für Cybersicherheit
  - Schulung, Überwachung & Einbindung in Entscheidungsprozesse



Status Quo

- Umsetzung bis 17. Oktober 2024
- 19 Mitgliedsstaaten haben noch keine Umsetzung mitgeteilt (u.a. Deutschland)

NIS2 Betroffenheitsprüfung

Wichtige Frage: Wen betrifft es

Zentrale Rechtsgrundlagen

- § 28 BSIG-E 2024
- Art. 3 NIS2-RL

Was ist zu prüfen

- Fällt das Unternehmen in einen Sektor: KRITIS oder Geschäftstätigkeit (Anlage 1 und 2)
- Werden Schwellenwerte erreicht („size cap“)

NIS2 Betroffenheitsprüfung

Schwellenwerte

- Anzahl Mitarbeiter ODER
- Jahresbilanz UND (EU: ODER) Jahresumsatz
- Ggf. Hinzurechnung in Unternehmensstruktur (§ 28 Abs. 2 BSIG-E 2024/über Art. 2 Abs. 1 NIS2-RL Empfehlung 2003/362/EG)

Herausforderung:

- Diskontinuitätsgrundsatz
- Regelung der Hinzurechnung im deutschen Entwurf „unglücklich“ umgesetzt

Fazit

Richtung ist klar

Pflichten sind klar

Betroffenheit im Wesentlichen klar

KI-Verordnung

Keine Umsetzung in nationales Recht erforderlich

Ziel

Schutz der Grundrechte natürlicher Personen im Zusammenhang mit dem Einsatz von künstlicher Intelligenz und die Förderung von Investitionen und Innovationen im KI-Bereich innerhalb der EU

Klassifizierung (Art. 6 und Anhang 3)

KI-Systeme werden nach Risikoklassen eingestuft:

🔴 Hochrisiko-KI-Systeme

- z. B. autonome Fahrzeuge, Kreditwürdigkeitsprüfung, kritische Infrastrukturen

➢ Strenge Anforderungen & Aufsichtspflichten

🟡 Geringeres Risiko

- z. B. Chatbots, Empfehlungssysteme

➢ Grundlegende Transparenzpflichten

📌 Ziel: Schutz von Sicherheit, Grundrechten & Vertrauen durch abgestufte Regulierung

Akteure (Art. 2)

- Anbieter (in Verkehr bringen oder in Betrieb nehmen)
- Betreiber
- Einführer und Händler
- Produkthersteller
- Bevollmächtigte von Anbietern
- Betroffene Personen

Rechtliche Definition „KI-System“ (Art. 3 Abs. 1 KI-VO)

Um festzustellen, ob ein Produkt als KI-System im Sinne dieser rechtlichen Definition gilt, ist zu prüfen, ob es:

- ist maschinengestützt,
- arbeitet selbstständig,
- kann sich nach dem Einsatz anpassen,
- beeinflusst die Umwelt durch seine Leistungen

Was gilt für Hersteller/Entwickler/Anbieter (Art. 16 – 23)

Technische & organisatorische Anforderungen:

✅ Risikomanagementsystem
- Identifikation, Analyse & Minderung von Risiken

📊 Datenqualität & -governance
- Repräsentative, fehlerfreie und relevante Trainingsdaten

📝 Technische Dokumentation
- Nachvollziehbarkeit & Transparenz der Systeme

⚙️ Protokollierungspflichten
- Automatisierte Aufzeichnungen zur Nachverfolgbarkeit

🧪 Transparenz & Nutzerinformationen
- Klare Hinweise für Anwender über Funktionsweise & Einsatz

🛠️ Menschliche Aufsicht
- Systeme müssen durch Menschen überwachbar & steuerbar bleiben

🛡️ Robustheit, Sicherheit & Genauigkeit
- Schutz vor Manipulation und Fehlfunktionen

Was gilt im Betrieb

Technisch-organisatorische Maßnahmen:

- ✅ Risikomanagementsystem (Art. 9)
- 📊 Datenqualität & Governance (Art. 10)
- 📝 Technische Dokumentation & Logfiles (Art. 11 & 12)
- 👁️ Transparenz & menschliche Aufsicht (Art. 13, 14 & 52)
- 🛡️ Robustheit, Cybersicherheit & Korrekturmöglichkeiten (Art. 15 & 25)
- 🚨 Meldepflicht bei schwerwiegenden Vorfällen (Art. 61)

Was gilt für Betreiber (Art. 26)

🧠 KI-Kompetenz aufbauen
- Schulung & Sensibilisierung der Mitarbeitenden (Art. 4)

📘 Anbietervorgaben einhalten
- Beachtung von Betriebsanleitungen & technischen Vorgaben (Art. 26 Abs. 1)
- Einhaltung von DSGVO & UrhG (TOMs)

👁️ Menschliche Aufsicht sicherstellen
- Nur geschultes, kompetentes & befugtes Personal (Art. 26 Abs. 2)

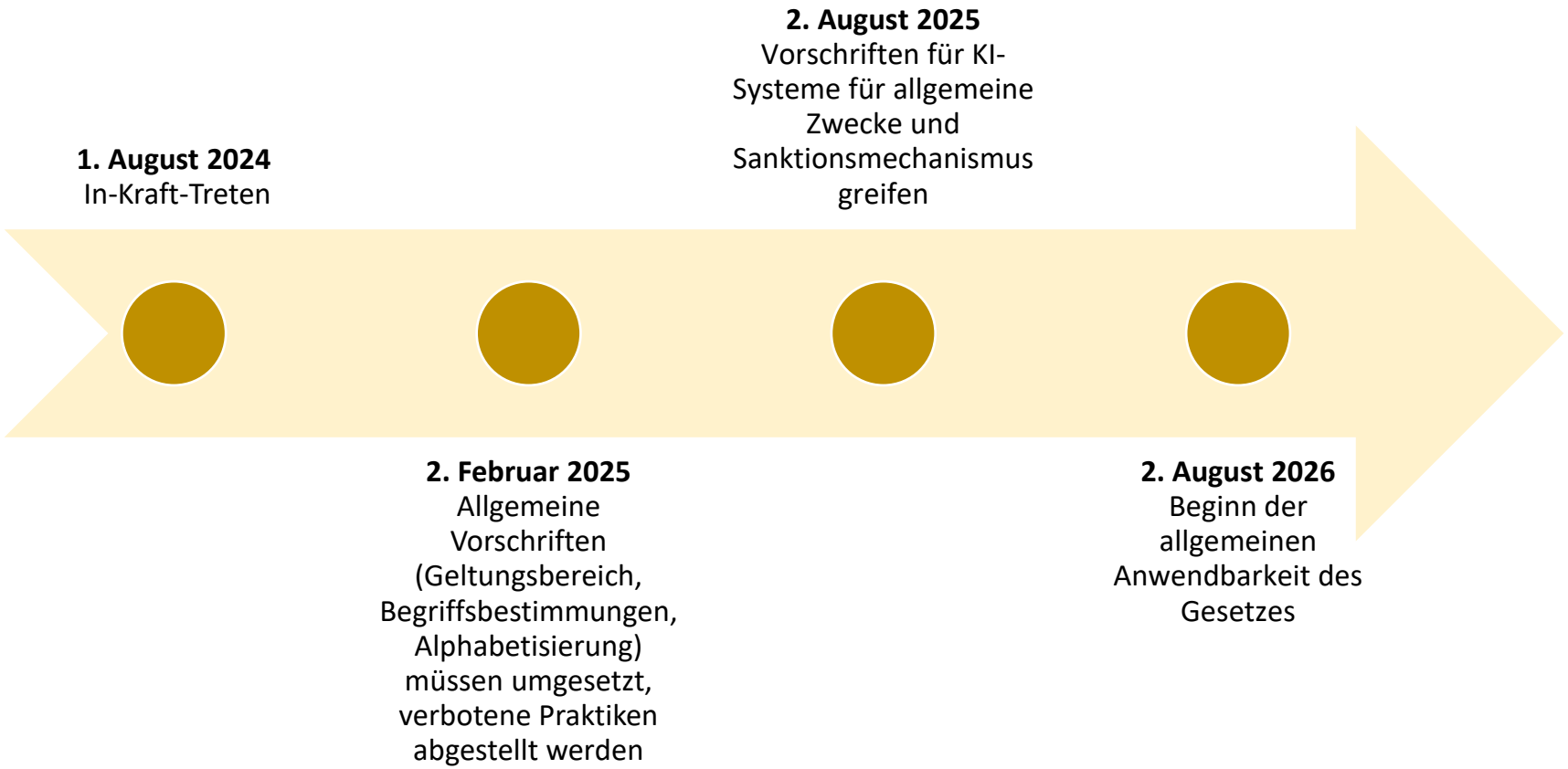
🚨 Unverzügliche Meldung bei Risiken
- Bei Gesundheits- oder Sicherheitsgefahr: Meldung an Aufsicht & Hersteller, ggf. Betriebsstopp (Art. 26 Abs. 5)

🗂️ Logfiles dokumentieren & aufbewahren
- Nachvollziehbarkeit sicherstellen (Art. 26 Abs. 6)

🔍 Transparenz & Grundrechte-Folgenabschätzung
- Info an Behörden & Betroffene gemäß DSGVO (Art. 26 Abs. 7 & Art. 27)

🤝 Kooperation mit Aufsichtsbehörden
- Pflicht zur Zusammenarbeit (Art. 26 Abs. 12)

Zeitplan


1. August 2024
In-Kraft-Treten
2. Februar 2025
Allgemeine Vorschriften (Geltungsbereich, Begriffsbestimmungen, Alphabetisierung) müssen umgesetzt, verbotene Praktiken abgestellt werden
2. August 2025
Vorschriften für KI-Systeme für allgemeine Zwecke und Sanktionsmechanismus greifen
2. August 2026
Beginn der allgemeinen Anwendbarkeit des Gesetzes

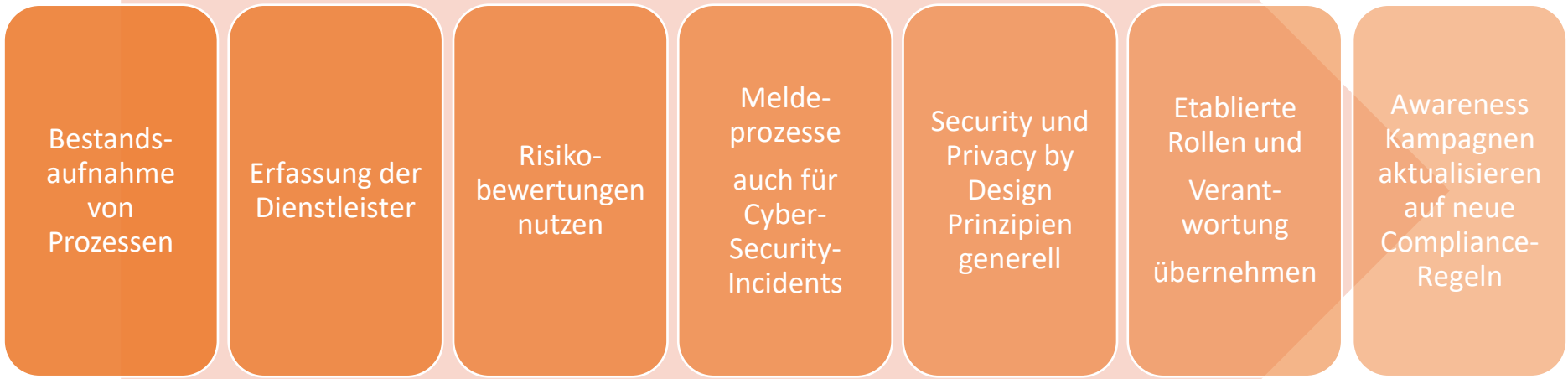
Wrap-Up

Wie kann man das zusammenfassen

Gemeinsame Anforderungen der Regulierungen

- Technische und organisatorische Maßnahmen
- Verpflichtung zur Vorfallmeldung an zuständige Stellen
- Verfolgen eines risikobasierten Ansatzes
- Dokumentations- und Nachweispflichten
- Verantwortung der Unternehmensführung

Update und gemeinsame Managementprozesse



Was bleibt hängen?
Fazit in Kürze

- NIS2 und die KI-Verordnung bringen **klare Anforderungen** an
  - Sicherheit
  - Transparenz
  - Organisation
  - Dokumentation
- Besonders betroffen: **Anbieter digitaler Infrastrukturen & Systeme mit KI-Komponenten**
- Der **regulatorische Rahmen** schafft neue Chancen – aber erfordert auch strukturelle Vorbereitung

Umsetzung erfordert abgestimmtes Handeln auf mehreren Ebenen

- **Organisatorisch**: Risikomanagement, Meldeprozesse, Aufsichtspflichten
- **Technisch**:
  - z. B. Logging, Monitoring, Schwachstellenmanagement, Schutzmechanismen
  - Hier leisten Anbieter von Cybersecurity-Lösungen einen zentralen Beitrag
- **Juristisch**: Einordnung, Compliance, Dokumentation, Verträge

👉 Rechtliche Beratung unterstützt bei der Integration dieser Anforderungen in Prozesse und Produkte – an der Schnittstelle zwischen Recht & Technik.

Ausblick und Abspann

Regulierung ist Realität – aber das Glück trifft den gut vorbereiteten.
Lassen Sie uns ins Gespräch kommen!

Diane Frank
diane.frank@schmid-frank.de