Deutsche Stiftung für Recht und Informatik

Digitale Resilienz durch Open-Source?

Rechtliche Handlungsspielräume in einer vernetzten Welt

Dr. Hendrik Schöttle
Osborne Clarke

Herbstakademie 2025

Übersicht

I. **Rechtlicher Rahmen**
- Überblick
- Cyber Resilience Act
- NIS-2-Richtline
- Data Act

II. Open Source als Mittel zur Resilienz

III. Vertragsgestaltung
- Allgemeine vertragliche Vereinbarungen
- Regelungen bezüglich Open-Source-Software

IV. Key Takeaways

A. Rechtlicher Rahmen | Überblick

- **Cyber Resilience Act (CRA)**:
  - **Ziel**: IT-Sicherheit für Produkte mit digitalen Elementen
  - **Stand**: In Kraft seit 10. Dezember 2024; Meldepflichten ab 11. September 2026; volle Geltung ab 11. Dezember 2027
- **NIS-2-Richtlinie**:
  - **Ziel**: IT-Sicherheit für kritische Infrastrukturen
  - **Stand**: In Kraft, Umsetzung in den Mitgliedstaaten bis zum 17. Oktober 2024, in Deutschland bisher noch nicht umgesetzt; Gesetzentwurf des NIS-2UmsuCG am 2. Oktober 2024 durch Neuwahlen im Februar 2025 überholt; Regierungsentwurf eines neuen NIS-2UmsuCG wurde am 30. Juli 2025 vom Bundeskabinett beschlossen und soll noch 2025 in Kraft treten
- **Data Act**:
  - **Ziel**: Schaffung eines Binnenmarktes für Daten und das Aufbrechen von Datensilos; enthält verbindliche Vorgaben zur Interoperabilität und Anbieterwechselbarkeit
  - **Stand**: In Kraft seit 11. Januar 2024; Geltung ab 12. September 2025

Cyber Resilience Act | Regulatorische Anforderungen

- **Konformität & Nachweise**
  - Laufende Risikobewertung und Dokumentation (Art. 13 Abs. 2 und 3, Art. 32 CRA): Im Regelfall Selbstbewertung; Fremdbewertung bei Klasse II oder kritischen Produkten
  - EU-Konformitätserklärung (Art. 13 Abs. 12, 28 Abs. 1, 32 CRA) und CE-Kennzeichnung (Art. 13 Abs. 12, 29, 30 Abs. 1–4) und Cybersicherheitszertifizierung, falls geeignetes Schema verfügbar (Art. 32 Abs. 1 lit. d, Art. 27 CRA)
- **Produktgestaltung**
  - Freiheit von bekannten Schwachstellen (Art. 6, 13 Abs. 1, Anhang I Teil I Abs. 2 lit. a CRA)
  - Regelmäßige Sicherheitsupdates und Möglichkeit zur Update-Verschiebung durch Nutzer (Anhang I Teil I Abs. 2 lit. c CRA)
  - Sichere Standardkonfiguration (Anhang I Teil I Abs. 2 lit. b CRA)
  - Datenschutzmaßnahmen (Anhang I Teil I Abs. 2 lit. d–f CRA)
  - Software-Stückliste (SBOM): Auflistung sämtlicher in das Produkt integrierter Komponenten (Art. 31 Abs. 1 i.V.m. Anhang VII Nr. 8 CRA)
- **Meldungen**
  - Binnen 24 Stunden Meldung an zuständige Behörde, wenn Schwachstellen ausgenutzt wurden oder wenn es zu sicherheitsrelevanten Vorfällen kommt
  - Nachmeldung binnen 72 Stunden an zuständige Behörde
  - Abschlussbericht binnen 14 Tagen bzw. eines Monats (Art. 14 CRA)
  - Meldepflicht an Nutzer (Art. 14 Abs. 8 CRA) und ggf. an Komponentenhersteller, soweit Drittkomponenten betroffen sind (Art. 13 Abs. 6 CRA)

NIS-2-Richtlinie | Regulatorische Anforderungen

- **Technische und organisatorische Maßnahmen**: Systematisches Risikomanagement; reicht von regelmäßigen Cyber Security Assessments, über Notfallpläne, Incident-Response, bis hin zur „Cyberhygiene“ (Art. 21 Abs. 1 und 2 NIS-2-RL)
- **Meldepflichten bei Sicherheitsvorfällen**: Wie bei CRA, Erstmeldung binnen 24 Stunden an zuständige Behörde; gefolgt von einem vollständigen Bericht binnen 72 Stunden; und einem Abschlussbericht binnen eines Monats (Art. 23 NIS-2-RL)
- **Lieferkettensorgfalt**:
  - Supply chain security policy muss etabliert werden, welche Direktlieferanten und Dienstleister berücksichtigt (Art. 21 Abs. 2 lit. d NIS-2-RL)
  - Insbesondere lieferantenbezogener Schwachstellen und Cybersecurity-Praktiken sind zu berücksichtigen (Art. 21 Abs. 3 NIS-2-RL)
  - Wichtig für Vertragsgestaltung
- **Authentifizierung und Zugriffsschutz**:
  - Verpflichtung zur Einführung von Multi-Faktor-Authentifizierung und rollenbasierter Zugriffskontrolle (Art. 21 Abs. 2 lit. I und j NIS-2-RL)
  - Vertraglich zu berücksichtigen, z.B. in Service-Level-Agreements, IT-Betriebsverträgen oder AGB

Data Act | Regulatorische Anforderungen

- **Interoperabilität und Anbieterwechsel**: Anbieter müssen alle vertraglichen und technischen Hindernisse beseitigen, die einen Wechsel erschweren und dürfen dabei keine Maßnahmen ergreifen, die den Anbieterwechsel behindern (Art. 23 lit. a–d Data Act)
- **Vorgaben für Verträge**: Kunden muss es grundsätzlich ermöglicht werden zu einem anderen Datenverarbeitungsdienst zu wechseln; verbindliche Übergangsfrist von höchstens 30 Kalendertagen (Art. 25 Abs. 2 lit. a Data Act); Kündigungsfrist für die Einleitung eines Wechsels darf zwei Monate nicht überschreiten (Art. 25 Abs. 2 lit. d Data Act)
- **Funktionale Äquivalenz**: Anbieter müssen Nutzer technische Mittel inkl. Dokumentation und unterstützender Funktionen bereitstellen, damit beim neuen Anbieter dieselben Funktionen nutzbar sind (Art. 30 Abs. 1 Data Act)
- **Entgeltverbot**: Grundsätzlich dürfen für Datenexport/Anbieterwechsel ab dem 12. Januar 2027 keine Entgelte verlangt werden; bis dahin kann nur der Ersatz von Kosten für nur eng begrenzte, tatsächlich angefallene Drittaufwände verlangt werden
- **Transparenz**: Unter anderem Offenlegung technischer Voraussetzungen, unterstützter Formate, Tools und Prozesse zur Anbieterwechselbarkeit (Art. 26 lit. a und b Data Act)
- **Schutz vor unrechtmäßigem staatlichem Zugriff**: Angemessene technische, organisatorische und rechtliche Maßnahmen, inkl. vertraglicher Zusagen zu Datenlokalisierung und Zugriffstransparenz (Art. 32 Abs. 1 und 2 Data Act)

Übersicht

I. Rechtlicher Rahmen
- Überblick
- Cyber Resilience Act
- NIS-2-Richtline
- Data Act

II. Open Source als Mittel zur Resilienz

III. Vertragsgestaltung
- Allgemeine vertragliche Vereinbarungen
- Regelungen bezüglich Open-Source-Software

IV. Key Takeaways

II. Open-Source als Mittel zur Resilienz

- **Vorteile**
  - **Transparenz & Auditierbarkeit**: Offener Code/Standards ermöglichen schnellere Identifikation/Behebung von Sicherheitslücken
  - **Geringerer Vendor-Lock-in**: Datenportabilität, offene Formate/Schnittstellen, leichterer Anbieterwechsel
  - **Service-Angebot**: Wahlfreiheit bei Dienstleistern aufgrund offener, dezentraler Struktur von Open-Source Projekten
  - **Weniger Abhängigkeiten**: Weniger Bindung an Hersteller, da Kontrolle über Code, Schnittstellen und Roadmap nicht exklusiv beim Hersteller bleiben
- **Nachteile**
  - **Haftung/Gewährleistung**: Typischerweise weitgehender Haftungs- und Gewährleistungsausschluss; individuelle vertragliche Absicherung nötig
  - **Wartungs- und Pflegerisiken**: Manche, auch kritischer Open-Source-Projekte wurden oder werden nur von wenigen Personen gepflegt (z.B. OpenSSL)
  - **Plattformabhängigkeiten**: Konzentration auf einzelne Repository-Plattformanbieter, insbesondere GitHub
  - „**Pseudo-OSS**“: Viele Open-Source Projekte sind nur auf dem Papier quelloffen; eine unabhängige Community fehlt und Kunden sind faktisch an Hersteller gebunden. Dann gehen Vorteile von OSS verloren

Übersicht

I. Rechtlicher Rahmen
- Überblick
- Cyber Resilience Act
- NIS-2-Richtline
- Data Act

II. Open Source als Mittel zur Resilienz

III. Vertragsgestaltung
- Allgemeine vertragliche Vereinbarungen
- Regelungen bezüglich Open-Source-Software

IV. Key Takeaways

III. Vertragsgestaltung | Wichtige Regelungen

Allgemeine vertragliche Vereinbarungen (1/2)

- **Stand der Technik**: Vereinbarung, dass Software dem Stand der Technik entspricht und frei von bekannten Schwachstellen ist
- **Zertifizierungen & Nachweise** (z.B. ISO/IEC 27001, ISO 27018, Common Criteria, BSI C5, TISAX, ISO/IEC 22301)
- **Software Bill of Materials (SBOM)**: SBOM sollte im Hinblick auf Art. 9 Abs. 2 lit. e CRA Vertragsbestandteil sein; zudem aus lizenzrechtlicher Sicht erforderlich
- **Konformitätsunterlagen auf Anforderung**: EU-Konformitätserklärung, CE-Kennzeichnung, begleitende technische/Sicherheitsdokumentation
- **Sicherheitsupdates**: Vertragliche Pflicht zu Sicherheitsupdates und Pflege über die Vertragslaufzeit
- **Dokumentationspflichten**: Vorlage von Konformitätserklärungen, CE-Kennzeichnung und weitere begleitende Dokumentation vertraglich zu vereinbaren
- **Meldepflichten**: Kooperationspflichten im Hinblick auf Meldungen von Sicherheitsvorfällen
- **Meldeverfahren**: Prozess sollte vertraglich vereinbart werden, insbesondere Ansprechpartner und Fristen

III. Vertragsgestaltung | Wichtige Regelungen

Allgemeine vertragliche Vereinbarungen (2/2)

- **Auditierbarkeit**: Recht zum Audit der Softwarelösung und Einhaltung vertraglich vereinbarter Sicherheits- und Compliance-Anforderungen sollte vertraglich vereinbart werden.
- **Software-Escrow**: Hinterlegung des Quellcodes und aller essenzieller Informationen für die Weiterbetrieb der Software für den Fall der Geschäftsaufgabe oder Insolvenz
- **Transit- und Exitklauseln**: Auch wenn teilweise von Data Act abgedeckt, sollten Regelungen zum Providerwechsel vereinbart werden, um Weiterbetrieb der Software bei einem Anbieterwechsel zu gewährleisten
- **Service Levels**: Verfügbarkeit, Wiederherstellungszeiten, Wiederanlaufpunkte und Reaktionszeiten sollten vertraglich abgesichert werden.
- **Business Continuity/Desaster Recovery**: Notfallmechanismen und Redundanzen sowie Backup-Regelungen

III. Vertragsgestaltung | Wichtige Regelungen

Regelungen bezüglich Open-Source-Software (1/2)

Zusätzlich zu den allgemeinen Regelungen:

- **Dokumentation und Code-Qualität**: Vertragliche Standards (bezahlter Weiterentwicklungen) festlegen, gerade bei ehrenamtlichen Projekten
- **Open-Source-Compliance**: Zertifizierung nach OpenChain-Standard (ISO/IEC 5230) festlegen sowie Bereitstellung von Updates
- **Gewährleistung und Support**: Ausdrückliche Regelung erforderlich, da Open-Source-Software üblicherweise nicht mit vertraglichen Gewährleistungsansprüchen einhergeht
- **Mitwirkungspflichten zentraler Entwickler**: Bestimmung eines Core-Maintainers für Entwicklungs- oder Prüfprozesse

III. Vertragsgestaltung | Wichtige Regelungen

Regelungen bezüglich Open-Source-Software (2/2)

- **Upstreaming**:
  - Vertragliche Rückgabeverpflichtung eigener Änderungen an die Open-Source-Community
  - Verhindert, dass der Kunde eigene Projekte „forkt“ und dadurch von der Community-Maintenance abkoppelt
- **Drittkomponenten**:
  - In der Regel empfiehlt es sich nicht, vertraglich pauschale Freigabeerfordernisse zu vereinbaren, da dies schnell zur operativen Belastung werden kann
  - Nur sinnvoll handhabbar, wenn ein gut ausgestattetes Open-Source Program Office vorhanden ist
  - Allow Lists oder Deny Lists sind im Einzelfall besser geeignet
  - Copyleft-Lizenzen pauschal zu verbieten ist weder praxistauglich noch notwendig, da dies mit einem Ausschluss eines signifikanten Teils von Open-Source-Software einhergeht (z.B. der Einsatz von Linux als Betriebssystem)

Übersicht

I. Rechtlicher Rahmen
- Überblick
- Cyber Resilience Act
- NIS-2-Richtline
- Data Act

II. Open Source als Mittel zur Resilienz

III. Vertragsgestaltung
- Allgemeine vertragliche Vereinbarungen
- Regelungen bezüglich Open-Source-Software

IV. Key Takeaways

IV. Key Takeaways

- Digitale Resilienz ist weder Selbstläufer noch Selbstzweck und muss **aktiv gestaltet** und vertraglich abgesichert werden
- Der Gesetzgeber rückt das Thema Digitale Resilienz zunehmend in den Fokus. **Wichtige allgemeine Vertragsregelungen zum Thema Sicherheit**:
  - Pflicht zu Sicherheitsupdates
  - Mitwirkung bei diversen Meldepflichten
  - Auditierbarkeit
- **Open-Source-Software** kann Resilienz stärken. **Vertraglich** sollten insbesondere die folgenden Punkte geregelt werden:
  - Standards zu Dokumentation und Code
  - Gewährleistung und Support
  - Nutzung von Drittkomponenten

Kontakt

Dr. Hendrik Schöttle
Rechtsanwalt | Partner | Fachanwalt für IT-Recht
T +49 89 5434 8046
M +49 175 2686271
E hendrik.schoettle@osborneclarke.com