HSW | RECHTSANWÄLTE
HARDER SEDLMEIER WEITZEL

4. Mandanten-Seminar – 5. Mai 2026

Neue Fallstricke im Wirtschaftsrecht

HSW | RECHTSANWÄLTE
HARDER SEDLMEIER WEITZEL

NIS2 und CRA – Oft überzogene Anforderungen an die Lieferkette

Dr. Christian Weitzel

Setting the Stage

- Die **DSGVO** – 2016 ein großer Aufreger
  - Jahre zuvor intensive Vorbereitung in allen Firmen
  - Aufwendige Vorbereitung in großen Projektteams
  - Bis heute ein „großes“ Compliance-Thema
- Die **DORA** 2022 (in Kraft ab 2023) erregte weniger Gemüter
  - Teils geringer Vorbereitungsaufwand („keine Mehrkosten bitte“!)
  - Meist nur halbherzige Umsetzung
  - Bis heute keine Sanktionen durch die BaFIN
- **CRA** und **NIS2** wurden schon argwöhnischer beäugt
  - Reger Austausch in juristischen Fachkreisen
  - In großen Firmen enorm aufwendige Vorbereitung
  - Im Mittelstand großteils ignoriert oder vernachlässigt

Worum geht es bei NIS2 und CRA?

- **Cyberresilienz-Verordnung (CRA) von 2024**
  - Verordnung (EU) 2024/2847 (…) über horizontale **Cybersicherheitsanforderungen** für Produkte mit digitalen Elementen (…)
  - Erwägungsgrund (1):
    „*Die **Cybersicherheit** bedeutet eine der größten Herausforderungen für die Union.*“
  - Soll **IT-Schwachstellen** in Produkten und mangelnde **Bereitstellung von Sicherheitsupdates** bekämpfen
- **NIS-2-Richtlinie von Dezember 2022**
  - Richtlinie (EU) 2022/2555 (…) über Maßnahmen für ein hohes gemeinsames **Cybersicherheitsniveau** in der Union
  - Soll Niveau der **Cyberresilienz** in der Union stärken

Überzogene Reaktionen

Teil 1: Vertragsnachträge

Nur bleibt es nicht bei Buzzwords …

- Schauen Sie mal, was ein großer Konzern allen Lieferanten als „3rd Party Security Agreement“ vorsetzen will:

> The Parties acknowledge that mitigating threats to information and network and information systems and ensuring the continuity of Services in the event of incidents is becoming essential to the functioning of supply chains and, in specific, to the cooperation of the Parties under the Agreement. ¶
>
> The Parties intend to mutually agree in this Annex ("**Data Security Annex**") on an appropriate level of information security and cyber resilience and to outline the security requirements to be implemented by **PROVIDER** to protect Company’s Information from loss of availability, authenticity, integrity or confidentiality, integrity and/or availability. ¶
>
> In order to comply with Company’s information and cybersecurity requirements, the Parties agree as follows: ¶

Nur bleibt es nicht bei Buzzwords …

- Schauen Sie mal, was ein großer Konzern allen Lieferanten als „3rd Party Security Agreement“ vorsetzen will:

> To ensure an appropriate level of Security of Network and Information Systems, **PROVIDER** must design, execute, and continuously monitor tailored technical, operational, and organizational measures according to information security standards (collectively defined as "**Information Security Management**").¶
>
> Information Security Management shall adhere to current, internationally recognized standards (such as ISO/IEC 270001, NIST Security Framework, and EU Commission Implementing Regulation (EU) 2024/2690 other regulations of the EU, as amended and updated from time to time), ensuring alignment with the latest industry best practices and complying with any updates to these standards ("**Information Security Standards**").¶

Nur bleibt es nicht bei Buzzwords …

- Schauen Sie mal, was ein großer Konzern allen Lieferanten als „3rd Party Security Agreement“ vorsetzen will:

IV. → **Asset Management**: **PROVIDER** shall establish and maintain controls and processes to ensure the identification and management of assets and appropriate protection responsibilities. **PROVIDER** shall maintain an up-to-date register of all assets involved in the processing of Company's Information and its operation (hardware, software, databases, and information systems), both internal and external. This includes: (a) inventory, (b) ownership, (c) acceptable use, (d) handling, (e) disposal, and (f) transfer. ¶

Nur bleibt es nicht bei Buzzwords …

- Schauen Sie mal, was ein großer Konzern allen Lieferanten als „3rd Party Security Agreement“ vorsetzen will:

VI. → **Application & Interface Security**: **PROVIDER** shall establish and maintain processes and controls which must ensure the secure development, testing, and release of systems, applications, and interfaces, encompassing: (a) requirements analysis and specification, (b) secure application architecture and interfaces, (c) secure software development lifecycle, (d) system engineering principles, (e) changes to software packages, (f) development environment, (g) outsourced development, (h) application testing and (i) applications approval.¶

Nur bleibt es nicht bei Buzzwords …

- Schauen Sie mal, was ein großer Konzern allen Lieferanten als „3rd Party Security Agreement“ vorsetzen will:

XIII. **Secure Administration (Privileged Access)**: **PROVIDER** shall establish and maintain processes and controls which must ensure secure authorized privileged access and prevent unauthorized privileged access to Company's Information and **PROVIDER**'s Network and Information Systems through the (a) management of privileged accounts, (b) recertification of privileged accounts, (c) activity monitoring, (d) session confidentiality and integrity, and (e) dedicated systems for administration.

So, weit so gut …

- … weil es bislang nur den Lieferanten betrifft.

So, weit so gut …

- … weil es bislang nur den Lieferanten betrifft.
- Aber jetzt diese Klausel:

6. Subcontracting

PROVIDER agrees to ensure that the engagement of each subcontractor and their subcontractors comply in all respects with the provisions of this Data Security Annex and that any law and regulatory requirements are not violated, and the **PROVIDER** remains the primary accountable party.

Und die Krönung des Ganzen zum Abschluss

- Ohne Worte:

7.→ Termination¶

Company may, in its sole discretion terminate the Agreement without penalty, by giving written notice to **PROVIDER,** if **PROVIDER** fails to perform any of its duties or responsibilities under this Data Security Annex. **PROVIDER** agrees that any violation of this Data Security Annex amounts to a material breach of the Agreement.¶

Überzogene Reaktionen

Teil 2: Vertragskündigungen

Auch die Kunden werden langsam wach

- Es sind nicht nur Auftraggeber, die Kopfschmerzen bereiten.

- Dr. Google und die angeblich so schlaue KI verleiten Kunden zur Kündigung von Wartungs- und Pflegeverträgen.
  - Angeblich müssten ja jetzt alle Mängel nach Gesetz beseitigt werden.
  - Und zwar kostenlos.
  - Und für die gesamte Nutzungsdauer eines Produktes.

Fake News

Das andere Extrem …

So abstrakt richtig, konkret aber falsch

- Open Source Software ist ausgenommen von den Pflichten nach CRA.
- CRA adressiert Schwachstellen (neudeutsch: Vulnerabilities).
- OSS in kommerzieller Software einzusetzen ist wirtschaftlicher Untergang
- SW-Pflegeverträge braucht es nicht mehr

Was stimmt – und was nicht?

Ein Blick ins Gesetz bringt mehr als jeder KI-Prompt …

So abstrakt richtig, konkret aber falsch (1/4)

- Open Source Software ist ausgenommen von den Pflichten nach CRA.
  - Aber nur, wenn sie nicht kommerziell bereitgestellt wird
  - Bei Integration in kommerzielle Software gelten alle Pflichten des CRA

  => Umgang mit OSS in der SW-Entwicklung wird grundlegenden Wandel erfahren.

- CRA adressiert Schwachstellen (neudeutsch: Vulnerabilities).
  - Aber nicht jede theoretische Schwachstelle ist zu melden und zu schließen
  - Nur aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle, Art. 14 (1) und (3) CRA.
  - Nur Schwachstellen im Endprodukt, nicht jede in mitgelieferter und teils ungenutzter OSS

So abstrakt richtig, konkret aber falsch (2/4)

- OSS in kommerzieller Software einzusetzen ist wirtschaftlicher Untergang.
  - Nein, sie wird nur aufwendiger und teurer.
  - SW-Entwicklung braucht Prozess der Schwachstellen-Überwachung:
    1. Alle OSS-Komponenten genau erfassen (SBOM!)
       - OSS-Komponenten, die sich nicht genau erfassen lassen, aus Produkt entfernen
    2. Alle Bestandteile regelmäßig auf Vulnerabilities prüfen
       - Geht wirtschaftlich vernünftig nur durch Automatisierung
    3. Bei Meldung einer Schwachstelle prüfen, ob diese aktiv genutzt wird
       - Im Zweifel lieber weitermachen mit der Prüfung
    4. Auswirkung der Schwachstelle innerhalb der Integration in Produkt prüfen:
       - Stellt sie dort eine Schwachstelle für den Anwender dar oder wirkt sie sich beim Betrieb des Produktes nicht aus (= ist sie dort nicht ausnutzbar?)

So abstrakt richtig, konkret aber falsch (3/4)

- OSS in kommerzieller Software einzusetzen ist wirtschaftlicher Untergang.
  - Nein, sie wird nur aufwendiger und teurer.
  - SW-Entwicklung braucht Prozess der Schwachstellen-Überwachung:
    4. Auswirkung der Schwachstelle innerhalb der Integration in Produkt prüfen:
       - Stellt sie dort eine Schwachstelle für den Anwender dar
         oder wirkt sie sich beim Betrieb des Produktes nicht aus (= ist sie dort nicht ausnutzbar?)
    5. Wenn ja, binnen 24 h Frühwarnung abgeben
    6. Wenn ja, ggf. Detailmeldung nachschieben
    7. Wenn ja, binnen 14 Tagen Patch anbieten

So abstrakt richtig, konkret aber falsch (4/4)

- SW-Pflegeverträge braucht es nicht mehr.
  - Nein, nur ein gewisser Anteil der Leistungen innerhalb von SW-Pflege muss kostenlos erbracht werden:
    => Bereitstellung von Patches für Sicherheitslücken i.S.d. Art. 14 CRA.
  - Ein umfangreich ausgestalteter SW-Pflegevertrag hat viele Leistungsbereiche (neudeutsch „service items“), die fast alle gegen Vergütung erbracht werden können.
  - Es braucht also lediglich einer geringfügigen Anpassung der SW-Pflegeverträge.
  - Die aber schon, sonst steigen Ihnen die Kunden aufs Dach!
- Sie müssen alle Lieferketten bis zum Ende abarbeiten.
  - Durchfilzen: Ja. Aber nicht bis zum Ende.
  - Gleichbehandeln: Nein

Zum Abschluss:

- **„Easy does it.“** oder **„One size fits all.“**

Zum Abschluss:

- „Easy does it.“ oder „One size fits all.“
  - Sie müssen nicht alle Sublieferanten in der Kette gleich behandeln.
  - Sie werden auch nicht alle gleich behandeln können.
  - Es braucht eine Klassifizierung der Lieferanten nach Risikogruppen
    - Beim der einen Firma vielleicht nur zwei oder drei Risikoklassen
    - Und bei einer großen fünf
  - Dann braucht es unterschiedliche „Behandlungspläne“ je nach Risikoklasse.

=> Einfach geht anders!

Ihre Berater zu diesen und anderen Fragen:

Bernd H. Harder

Rechtsanwalt

Dr. Johannes Sedlmeier, LL.M.

Rechtsanwalt
Fachanwalt für Arbeitsrecht

Maximilian Schimmelpfennig

Rechtsanwalt
Fachanwalt für Arbeitsrecht

Dr. Christian Weitzel

Rechtsanwalt
Fachanwalt für Informationstechnologierecht