

TeleTrust-interner Workshop

Berlin, 01.07.2025

Auswirkungen der neuen Produkthaftung für Software auf den Softwarevertrieb und die Vertragsgestaltung

Dr. Carsten Brodersen, HK2

Welche Haftung?

- **Öffentlich-rechtliche Haftung**
 - Aufsichtsbehördliche Sanktionen – nach DSGVO, KI-VO; usw.
- **Zivilrechtliche Haftung**
 - **Vertraglich:** Schuldrechtliche Gewährleistung zwischen Vertragsparteien (B2C)
 - **Außervertraglich: Gesetzliche Produkthaftung** nach EU-Produkthaftungsrichtlinie
 - **Verbraucher** vs. Hersteller (B2C)
 - **Verschuldensunabhängiger** Schadensersatz
 - Für kausal auf Produktfehlern basierenden **Personen-** und **Sachschaden**



Produkthaftungsrichtlinie 2.0: Worum geht's?

Modernisierung der Herstellerhaftung für fehlerhafte Produkte

- Alte Richtlinie stammt aus **1985**
- Anpassung an **Risiken digitaler Produkte** war erforderlich
 - **Software als Produkt** (SaaS, KI-Systeme usw.)
 - **Entwickler als Hersteller**
 - Prinzip: **Haftung** folgt **Kontrolle** über gesamten **Lebenszyklus** des Produkts
- **Richtlinie** in Kraft seit **9. Dezember 2024**
 - Gilt für **Produkte**, die **ab 9. Dezember 2026** in Verkehr gebracht werden
 - Richtlinie: Umsetzung im **nationalen Recht** erforderlich
(= Produkthaftungsgesetz)

Produktfehler & IT-Sicherheit

Gesetzliche IT-Sicherheitsvorgaben als Produktfehler

- Bekannte Sicherheitsaspekte schon **bei** Inverkehrbringen des Produkts
- Fortlaufender, angemessener Schutz **nach** Inverkehrbringen
 - **Prinzip: „Haftung folgt Kontrolle“**
 - Konkretisiert durch spez. Produktsicherheitsrecht: **Cyber Resilience Act (CRA)**
 - Pflicht: **Kostenlose** Bereitstellung von Sicherheitsupdates
 - **Supportfristen** für Sicherheitsupdates:
 - Grundsätzlich: **fünf Jahre**
 - Produkte mit **kürzerer Nutzungsdauer**: entsprechend „**voraussichtlicher**“ Nutzungsdauer

To-dos



Cybersecurity by
design



Cybersicherheitsrisiken
überwachen/beheben

IT-Sicherheit über den gesamten Lebenszyklus mitdenken und umsetzen

- Lifecycle-orientierte Produktplanung, –entwicklung und –beobachtung etablieren
- Updatefähigkeit technisch sicherstellen
- Updatefristen überprüfen
- „Misch-Updates“ (Funktion und Sicherheit) überdenken und korrekt aussteuern

To-dos

Haftungsrisiken absichern und Vertragspraxis anpassen

- **Verträge** und **AGB** sind anzupassen
 - **Leistungspflichten** für **Sicherheitsupdates** verbindlich regeln
 - Sicherheitsupdates vertraglich **unentgeltlich** und **fristgerecht** leisten
 - Haftungsausschlüsse **verboten**
 - **Parität** der **Leistungen** trotz Haftungsrisikos gewahrt?
- **Versicherungsschutz** anpassen
- **Kommunikation** und **Marketing** überprüfen

