

IT-SICHERHEITSRECHT ALS EIN GRUNDPFEILER DES GESUNDHEITSDATENRAUMS

Dr. Roman Schildbach

ByteLaw Rechtsanwälte,
Frankfurt am Main

Herbstakademie 2026

Vision des Gesundheitsdatenraums (EHDS) für 2030:



Jede neue Verfügbarkeit ist auch eine neue Angriffsfläche

Bildquelle: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

IT-Sicherheit als Grundbedingung für den Datenraum

- ▶ EHDS soll Datennutzung/-austausch & Forschung erleichtern
- ▶ Erfolg hängt vom Vertrauen der Bevölkerung ab
- ▶ Ein schwerwiegender Cyberangriff könnte Vertrauen nachhaltig erschüttern
- ▶ **IT-Sicherheit ist daher Funktionsbedingung des EHDS**
- ▶ **Kernfrage: Wie adressiert der Gesetzgeber dieses Risiko?**

Agenda

- 01 IT-Sicherheitsrecht des EHDS
- 02 Vorgaben bei der Primärnutzung
- 03 Regelungen der Sekundärnutzung
- 04 Praktische Bedeutung & Fazit

Der EHDS im Überblick

Primärnutzung

- ▶ Mehr digitaler Datenzugang für PatientInnen
- ▶ Mehr Datenaustausch
- ▶ Auch grenzüberschreitend

Sekundärnutzung

- ▶ Datenzugang für Forschung und Innovation
- ▶ Verpflichtende Datenbereitstellung
- ▶ Überwiegend staatlich organisierte Zugangsstrukturen

Gemeinsame Konsequenz:

Wo der Staat Datennutzung ermöglicht und organisiert, muss er die nötige IT-Sicherheit gewährleisten

IT-Sicherheit als zentrale Leitmotiv

- Erwägungsgrund 4 der EHDS-VO:
Schutzmaßnahmen, um ein hohes Maß an **Datenschutz**,
Sicherheit, **Vertraulichkeit** und **ethischer Nutzung**
sicherzustellen.

The EHDS aims to create a truly integrated European approach to health data management while maintaining strong privacy standards. It is founded on:

Trust

Data security

Transparency

Respect for people's rights



Primärnutzung: drei Regelungskomplexe

EHR-Systeme

- System zur Verarbeitung von Gesundheitsdaten bei Behandlung
- Betrifft auch private Marktakteure
- Produktsicherheit mit harmonisierten Komponenten, Dokumentation, Konformität und Marktüberwachung
- Neue Meldepflicht nach Art. 44 Abs. 7 UAbs. 1 EHDS-VO für schwerwiegende Vorkommnisse



detaillierte Regeln

Zugangsdienste

- Staatlich organisierte Datenzugänge für PatientInnen und health professionals
- Fokus auf Identitätsinfrastruktur
- Technische Ausgestaltung und Schutz der Infrastruktur bleiben weitgehend nachgelagerten **Durchführungsrechtsakten** überlassen



kaum Vorgaben im Sekundärrecht

MyHealth@EU

- Zentrale grenzüberschreitende Infrastruktur/Plattform
- Sicherheit, Vertraulichkeit und Cybersicherheit werden erst durch **Durchführungsrechtsakte** konkretisiert



Primärnutzung: Allgemeine Vorgaben

Art. 86 S. 1 EHDS-VO:

- ▶ Besonders hohes Maß an Schutz und Sicherheit als allgemeine Pflicht für die Mitgliedstaaten
- ▶ Erinnert an Art. 32 DSGVO als allgemeine IT-Sicherheitspflicht ohne spezielle Vorgaben

Art. 86 S. 2 EHDS-VO:

- ▶ Keine unionsrechtliche Pflicht zur Datenverarbeitung in der EU (Datenlokalisierung)
- ▶ Jedoch: Öffnungsklausel für Mitgliedstaaten
- ▶ Beispiel Deutschland: §393 Abs. 2 SGB V, wonach Clouddienste der Leistungserbringer der GKV einer Datenlokalisierungspflicht unterliegen (C5-Zertifizierung)

IT-Sicherheit bei der Sekundärnutzung

Was regelt die EHDS-VO konkret?

- ▶ Zugang über sichere Verarbeitungsumgebungen (Art. 73)
- ▶ Zugang nur für autorisierte Nutzer (Art. 73 Abs. 1 lit. a)
- ▶ Umfassende Protokollierung und Überwachung der Nutzung (Art. 73 Abs. 1 lit. c-e)
- ▶ Kontrolle von Datenausgaben und Exporten (Art. 73 Abs. 1 lit. f ff.)
- ▶ Interne und externe Audits (Art. 73 Abs. 3)
- ▶ Datenlokalisierungspflicht in der EU (Art. 87)

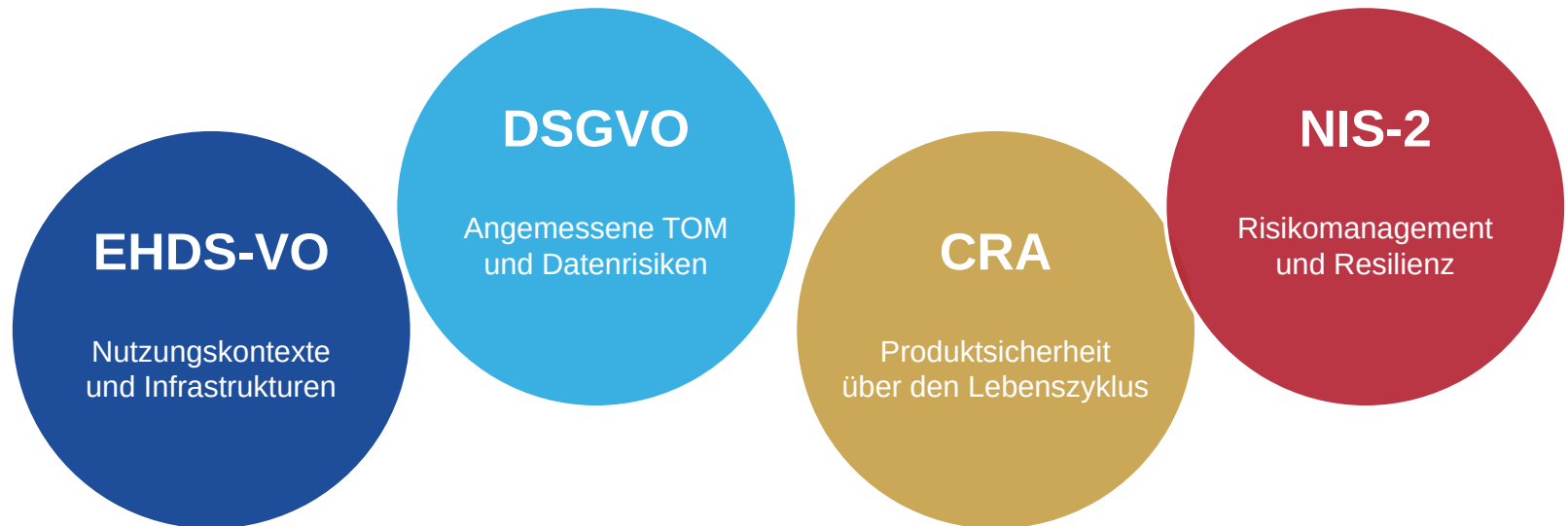
Was regelt die EHDS-VO kaum?

- ▶ Pflichten zu Information Security Management
- ▶ Konkreten Vorgaben zu Verschlüsselung
- ▶ Pentesting-Pflichten
- ▶ Patchmanagement-Pflichten
- ▶ Schulungspflichten von Personal zu IT-Sicherheit
- ▶ **Insgesamt:** Kaum spezifische Vorgaben zum Schutz vor externen Cyberangriffen

Die EHDS-VO kontrolliert den berechtigten Nutzer detaillierter als den externen Angreifer



Zusammentreffen mehrerer Regelwerke



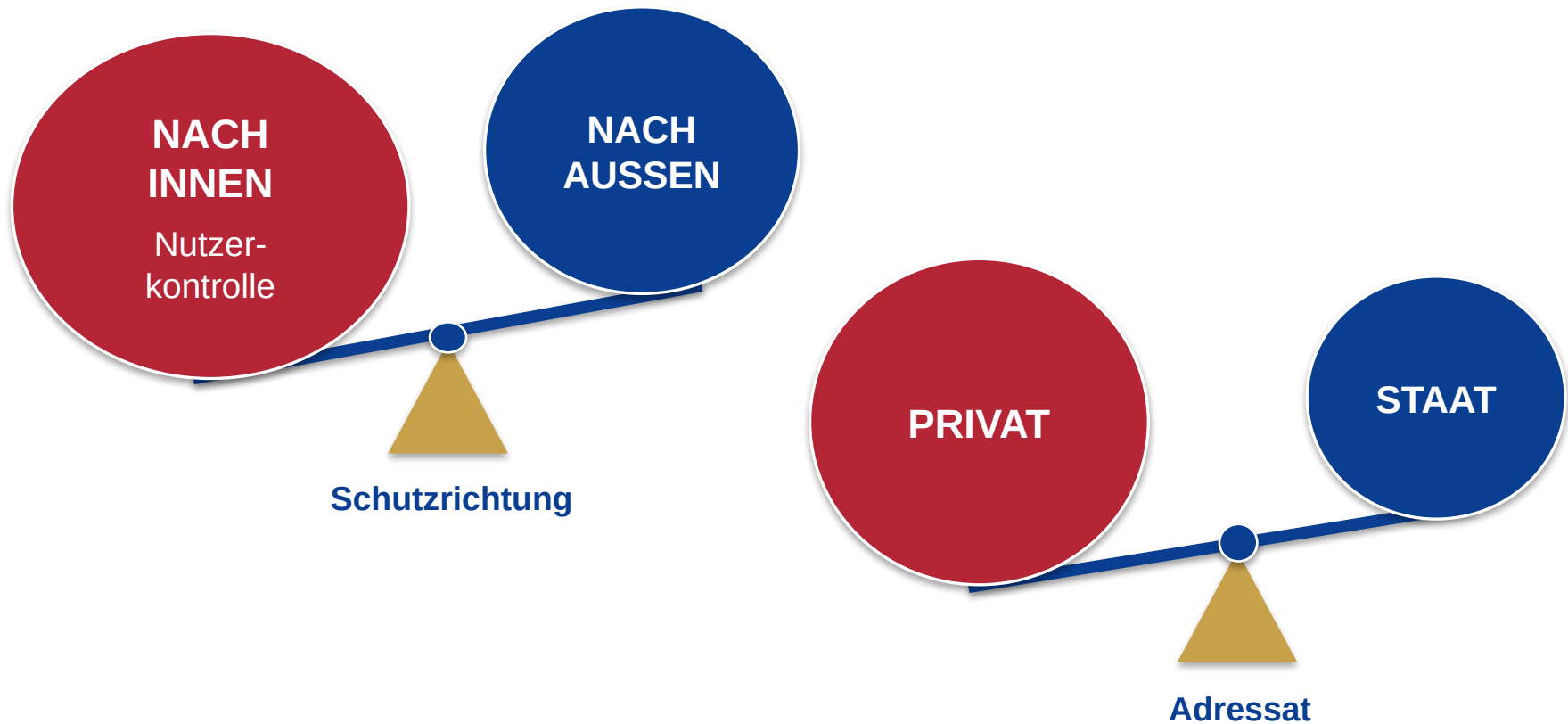
**Kumulative Pflichten möglich, Beispiel
Meldepflichten**

IT-Sicherheitsrecht des EHDS mit doppelter Schlagseite

mehr konkrete Regulierung



abstraktere Vorgaben



Ausblick auf die eigentliche Herausforderung

IT-Sicherheit endet nicht mit dem Inkrafttreten der EHDS-VO

Sie beginnt dort.

- ▶ Daueraufgabe
- ▶ Dauerfinanzierung
- ▶ Dauerüberwachung
- ▶ Daueranpassung

Immense staatliche Aufgabe in heterogenen und teils komplexen Gesundheitssystemen

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?