KI-Verordnung, Data Act, Cyber Resilience Act...

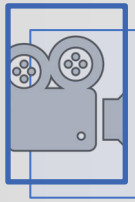
WELCHE VORSCHRIFTEN MUSS ICH ALS DSB AUßER DER DSGVO NOCH KENNEN?

PRIVACYXPERTS

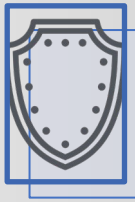
KI-Verordnung, Data Act, Cyber Resilience Act...

Ihr Referent: Rechtsanwalt Michael Rohrlich, Würselen – www.ra-rohrlich.de

niedergelassener **Rechtsanwalt**

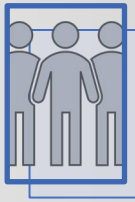


Video-Trainer u.a. bei LinkedIn Learning



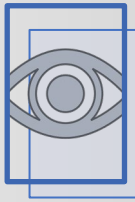
TÜV Süd zert. **Datenschutzbeauftragter** (DSB-TÜV)

geprüfter **Datenschutz-auditor** (Haufe)



HR Data Protection Manager (Beck)

Data Protection Risk Manager (FOM)



zert. **Informationssicherheits-beauftragter** (IHK)

zert. **IT-Grundschutz-Praktiker** (BSI)

zert. **Legal Prompt Engineer** (v. Fürstenberg)

Fachautor & Referent

PRIVACYXPERTS

KI-Verordnung, Data Act, Cyber Resilience Act...

🗎 Agenda:

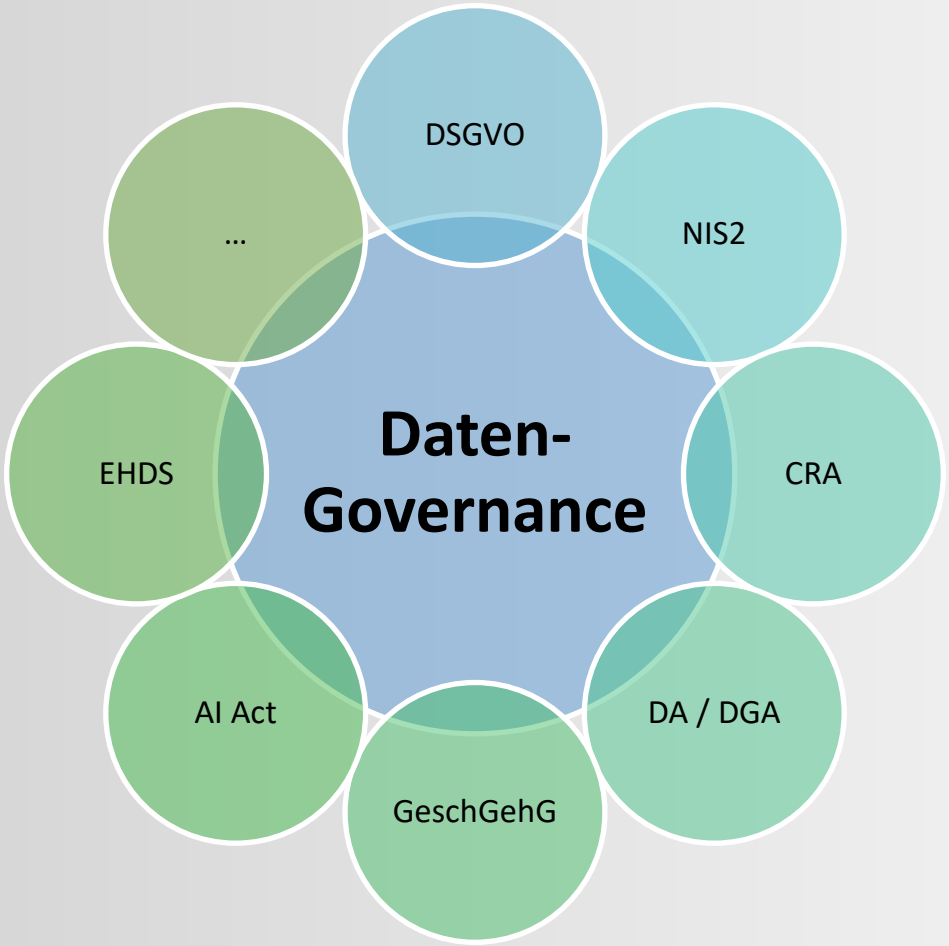
1. Einführung
2. KI-Verordnung
3. NIS2 / dt. NIS2-Umsetzungsgesetz
4. Cyber Resilience Act
5. Data Act
6. Geschäftsgeheimnisgesetz

PRIVACYXPERTS

1

Einführung

Einführung



PRIVACYXPERTS

2

KI-Verordnung

KI-VO

1. August 2024
- Inkrafttreten

2. Februar 2025
- allg. Vorschriften (Art. 1-3)
- Verbot bestimmter KI (Art. 5)
- KI-Kompetenz (Art. 4)

2. August 2025
- GPAI
- Notifizierungsstellen
- Governance
- Sanktionen

~~2. August 2026~~
- Hochrisiko-KI-Systeme (Art. 6, Anh. III)
- KI-Systeme, die nicht in die Hochrisiko-Klasse fallen
- **Transparenzpflichten weiterhin ab dem 2. August 2026!**

~~2. August 2027~~
- Hochrisiko-KI-Systeme (Art. 6, Anh. I)

„Digital Omnibus on AI“

→ 2. Dezember 2027

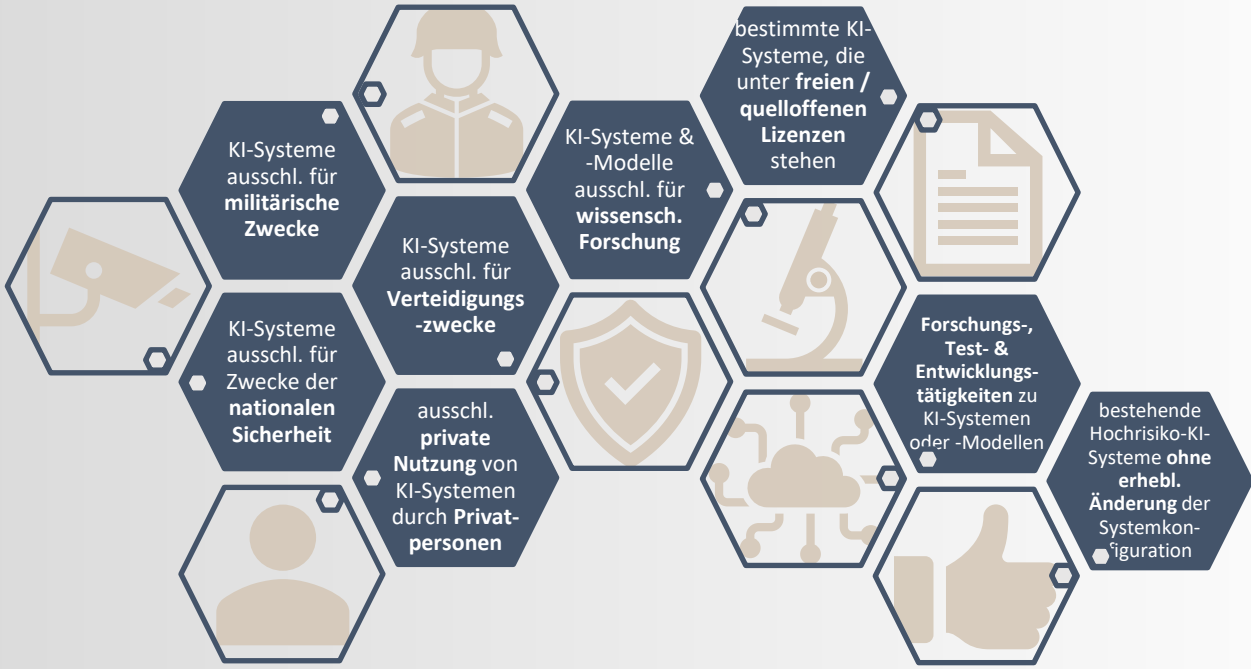
→ 2. August 2028

PRIVACY XPERTS

KI-VO

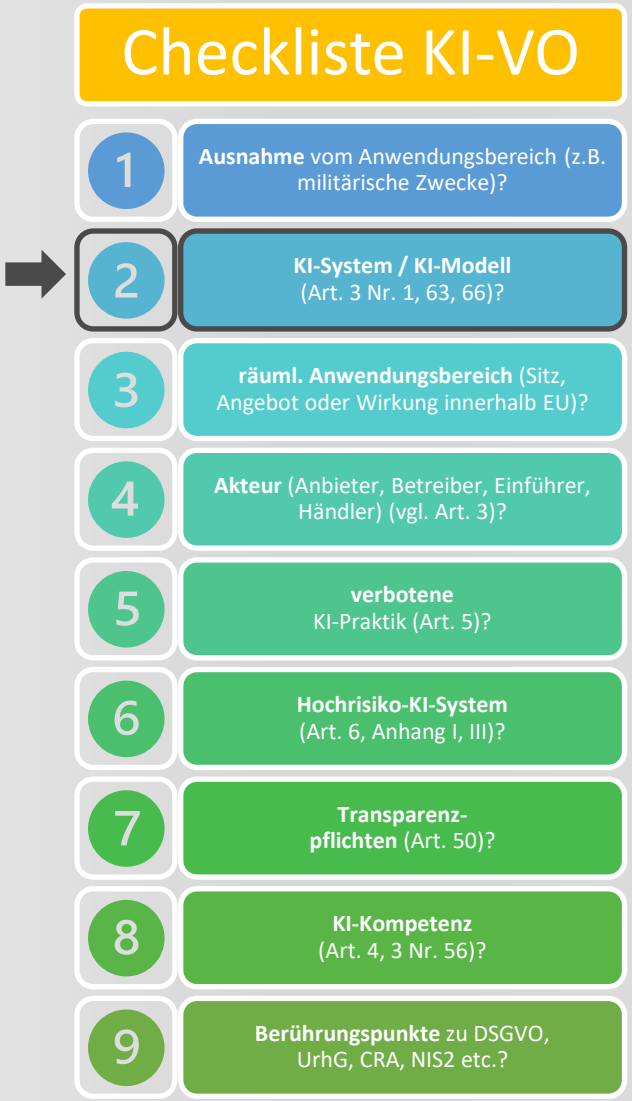
Checkliste KI-VO

1. **Ausnahme** vom Anwendungsbereich (z.B. militärische Zwecke)?
2. **KI-System / KI-Modell** (Art. 3 Nr. 1, 63, 66)?
3. **räuml. Anwendungsbereich** (Sitz, Angebot oder Wirkung innerhalb EU)?
4. **Akteur** (Anbieter, Betreiber, Einführer, Händler) (vgl. Art. 3)?
5. **verbotene** KI-Praktik (Art. 5)?
6. **Hochrisiko-KI-System** (Art. 6, Anhang I, III)?
7. **Transparenz-pflichten** (Art. 50)?
8. **KI-Kompetenz** (Art. 4, 3 Nr. 56)?
9. **Berührungspunkte** zu DSGVO, UrhG, CRA, NIS2 etc.?



PRIVACYXPERTS

KI-VO



- **Def. „KI-System“ (Art. 3 Nr. 1)**
- *„ein **maschinengestütztes** System, das für einen in unterschiedlichem Grad **autonomen Betrieb** ausgelegt ist und das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele **ableitet**, wie **Ausgaben** wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen **beeinflussen** können“*

PRIVACYXPERTS

KI-VO

Checkliste KI-VO

1. **Ausnahme** vom Anwendungsbereich (z.B. militärische Zwecke)?
2. **KI-System / KI-Modell** (Art. 3 Nr. 1, 63, 66)?
3. **räuml. Anwendungsbereich** (Sitz, Angebot oder Wirkung innerhalb EU)?
4. **Akteur** (Anbieter, Betreiber, Einführer, Händler) (vgl. Art. 3)?
5. **verbotene** KI-Praktik (Art. 5)?
6. **Hochrisiko-KI-System** (Art. 6, Anhang I, III)?
7. **Transparenz-pflichten** (Art. 50)?
8. **KI-Kompetenz** (Art. 4, 3 Nr. 56)?
9. **Berührungspunkte** zu DSGVO, UrhG, CRA, NIS2 etc.?

Niederlassungsprinzip

Betreiber von KI-Systemen, die sich in der EU befinden oder die ihren **Sitz** in der EU haben

Marktortprinzip

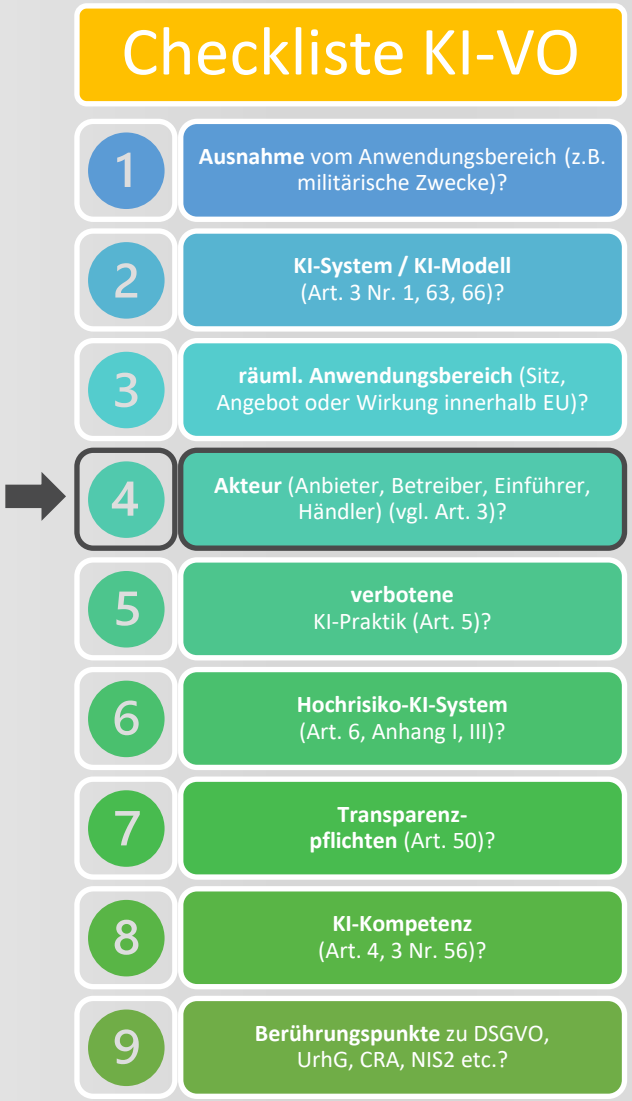
Anbieter, die KI-Systeme / GPAI in der EU **in Verkehr bringen oder in Betrieb nehmen**

extraterritoriale Wirkung

Anbieter / Betreiber von KI-Systemen, deren **Ausgabe** in der EU verwendet wird

PRIVACYXPERTS

KI-VO



- **Def. „Anbieter“ (Art. 3 Nr. 3)**
- *„eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck **entwickelt oder entwickeln lässt** und es unter ihrem **eigenen Namen** oder ihrer **Handelsmarke** in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke **in Betrieb nimmt**, sei es entgeltlich oder unentgeltlich“*

- **Def. „Betreiber“ (Art. 3 Nr. 4)**
- *„eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System **in eigener Verantwortung verwendet**, es sei denn, das KI-System wird im Rahmen einer **persönlichen** und nicht beruflichen Tätigkeit verwendet“*

PRIVACY XPERTS

KI-VO

„Digital Omnibus on AI“

neue Verbote:
„Nudification“-KI
und CSAM-KI

Checkliste KI-VO

1. **Ausnahme** vom Anwendungsbereich (z.B. militärische Zwecke)?
2. **KI-System / KI-Modell** (Art. 3 Nr. 1, 63, 66)?
3. **räuml. Anwendungsbereich** (Sitz, Angebot oder Wirkung innerhalb EU)?
4. **Akteur** (Anbieter, Betreiber, Einführer, Händler) (vgl. Art. 3)?
5. **verbotene** KI-Praktik (Art. 5)?
6. **Hochrisiko-KI-System** (Art. 6, Anhang I, III)?
7. **Transparenz-pflichten** (Art. 50)?
8. **KI-Kompetenz** (Art. 4, 3 Nr. 56)?
9. **Berührungspunkte** zu DSGVO, UrhG, CRA, NIS2 etc.?

KI mit allg. Verwendungs-zweck (engl.: general purpose AI, GPAI), z.B. ChatGPT

Verbotene KI-Praktiken (Art. 5)

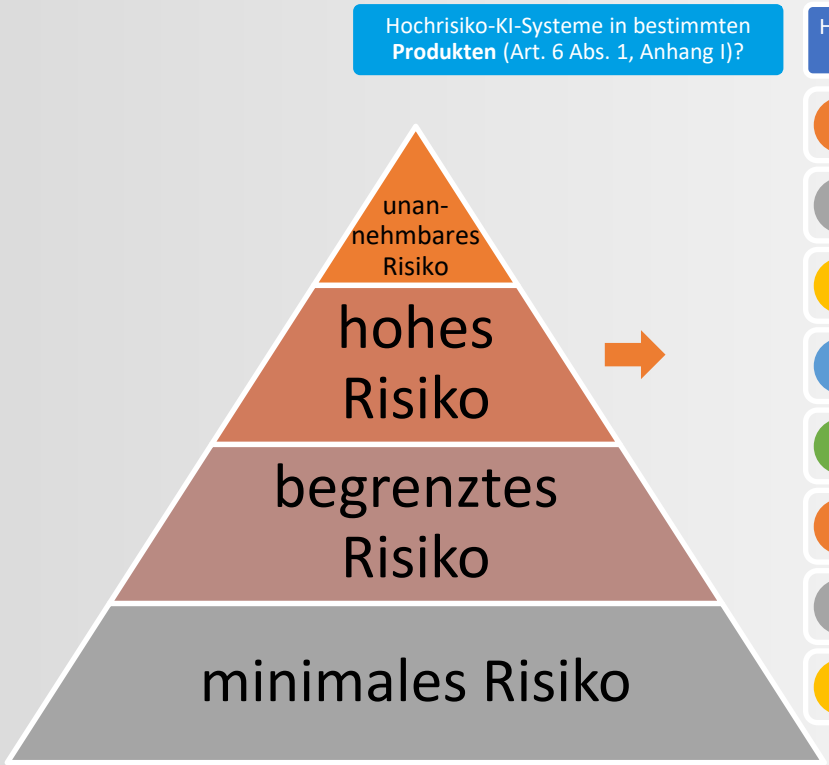
- unterschwellige Beeinflussung
- Ausnutzung der Schwäche oder Schutzbedürftigkeit von Personen
- biometrische Kategorisierung
- Bewertung des sozialen Verhaltens (Social Scoring)
- biometrische Echtzeit-Fernidentifizierungs-systeme
- Risikobeurteilung von natürlichen Personen
- Datenbanken zur Gesichtserkennung
- Ableitung von Emotionen natürlicher Personen in Schule, Uni, Büro…
- Analyse von aufgezeichnetem Bildmaterial

PRIVACY XPERTS

KI-VO

Checkliste KI-VO

1. **Ausnahme** vom Anwendungsbereich (z.B. militärische Zwecke)?
2. **KI-System / KI-Modell** (Art. 3 Nr. 1, 63, 66)?
3. **räuml. Anwendungsbereich** (Sitz, Angebot oder Wirkung innerhalb EU)?
4. **Akteur** (Anbieter, Betreiber, Einführer, Händler) (vgl. Art. 3)?
5. **verbotene** KI-Praktik (Art. 5)?
6. **Hochrisiko-KI-System** (Art. 6, Anhang I, III)?
7. **Transparenz-pflichten** (Art. 50)?
8. **KI-Kompetenz** (Art. 4, 3 Nr. 56)?
9. **Berührungspunkte** zu DSGVO, UrhG, CRA, NIS2 etc.?



Hochrisiko-KI-Systeme durch bestimmten **Zweck** (Art. 6 Abs. 2, Anhang III)?

1. **erlaubte Biometrie**
2. **KRITIS**-Verwaltung und -Betrieb
3. allg. und berufliche **Bildung**
4. **Beschäftigung**, Personalmanagement und Zugang zur Selbstständigkeit
5. Zugänglichkeit und Inanspruchnahme grundlegender **priv. und öffentl. Dienste & Leistungen**
6. **Strafverfolgung** (Lügendetektor, Profiling…)
7. **Migration**, Asyl und Grenzkontrolle
8. **Rechtspflege** (Justizbehörden) und demokratische Prozesse

PRIVACY XPERTS

KI-VO

Checkliste KI-VO

1. **Ausnahme** vom Anwendungsbereich (z.B. militärische Zwecke)?
2. **KI-System / KI-Modell** (Art. 3 Nr. 1, 63, 66)?
3. **räuml. Anwendungsbereich** (Sitz, Angebot oder Wirkung innerhalb EU)?
4. **Akteur** (Anbieter, Betreiber, Einführer, Händler) (vgl. Art. 3)?
5. **verbotene** KI-Praktik (Art. 5)?
6. **Hochrisiko-KI-System** (Art. 6, Anhang I, III)?
7. **Transparenz-pflichten** (Art. 50)?
8. **KI-Kompetenz** (Art. 4, 3 Nr. 56)?
9. **Berührungspunkte** zu DSGVO, UrhG, CRA, NIS2 etc.?

- **Transparenz- / Kennzeichnungspflicht für bestimmte KI-Systeme (Art. 50 Abs. 3, 3 Nr. 39,40)**
- *„Die Betreiber eines **Emotionserkennungssystems** oder eines **Systems zur biometrischen Kategorisierung** informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems und verarbeiten personenbezogene Daten gemäß [u.a. der DSGVO]. Diese Pflicht gilt nicht für gesetzlich zur **Aufdeckung, Verhütung oder Ermittlung von Straftaten** zugelassene KI-Systeme, die zur biometrischen Kategorisierung und Emotionserkennung im Einklang mit dem Unionsrecht verwendet werden, sofern geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.“*

- **Transparenz- / Kennzeichnungspflicht für Deepfakes (Art. 50 Abs. 4 S. 1-3, vgl. Def. in Art. 3 Nr. 60)**
- *„Betreiber eines KI-Systems, das **Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert**, die ein Deepfake sind, müssen **offenlegen**, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Diese Pflicht gilt nicht, wenn die Verwendung zur **Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten** gesetzlich zugelassen ist. Ist der Inhalt **Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms**, so **beschränken** sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte **in geeigneter Weise offenzulegen**, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.“*

- **Transparenz- / Kennzeichnungspflicht für News (Art. 50 Abs. 4 S. 4-5)**
- *„Betreiber eines KI-Systems, das **Text erzeugt oder manipuliert**, der **veröffentlicht** wird, um die Öffentlichkeit über **Angelegenheiten von öffentlichem Interesse** zu informieren, müssen **offenlegen**, dass der Text künstlich erzeugt oder manipuliert wurde. Diese Pflicht gilt nicht, wenn die Verwendung zur **Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten** gesetzlich zugelassen ist oder wenn die durch KI erzeugten Inhalte einem **Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle** unterzogen wurden und wenn eine natürliche oder juristische Person die **redaktionelle Verantwortung** für die Veröffentlichung der Inhalte trägt.“*

PRIVACYXPERTS

„Digital Omnibus on AI“

Abschwächen der Förderpflicht

KI-VO

Checkliste KI-VO

1. **Ausnahme** vom Anwendungsbereich (z.B. militärische Zwecke)?
2. **KI-System / KI-Modell** (Art. 3 Nr. 1, 63, 66)?
3. **räuml. Anwendungsbereich** (Sitz, Angebot oder Wirkung innerhalb EU)?
4. **Akteur** (Anbieter, Betreiber, Einführer, Händler) (vgl. Art. 3)?
5. **verbotene** KI-Praktik (Art. 5)?
6. **Hochrisiko-KI-System** (Art. 6, Anhang I, III)?
7. **Transparenz-pflichten** (Art. 50)?
8. **KI-Kompetenz** (Art. 4, 3 Nr. 56)?
9. **Berührungspunkte** zu DSGVO, UrhG, CRA, NIS2 etc.?

- **Def. „KI-Kompetenz“ (Art. 3 Nr. 56)**
- *„die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden“*

- **KI-Kompetenz (Art. 4)**
- *„Die Anbieter und Betreiber von KI-Systemen ergreifen **Maßnahmen**, um nach besten Kräften **sicherzustellen**, dass ihr **Personal und andere Personen**, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein **ausreichendes Maß an KI-Kompetenz** verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu **berücksichtigen** sind.“*

PRIVACYXPERTS

KI-VO

- Leitlinien der EU-Kommission zur Definition eines Systems der künstlichen Intelligenz (02/2025)
- Leitlinien der EU-Kommission zu verbotenen Praktiken der künstlichen Intelligenz (02/2025)
- Lebendiges Repository der EU-Kommission für KI-Kompetenz (01/2025)
- FAQ der EU-Kommission zu KI-Modelle mit allg. Verwendungszweck (03/2025)
- FAQ der EU-Kommission zur KI-Kompetenz (05-2025)
- Leitlinien für den Einsatz Künstlicher Intelligenz in der Bundesverwaltung (03/2026)
- BSI Test Criteria Catalogue for AI Systems in Finance (06/2025)
- „The Bridge Blueprint - Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim KI-Einsatz“ (u.a. vom HBfDI)
- BNetzA: Hinweispapier "KI-Kompetenzen nach Artikel 4 KI-Verordnung" (06/2025)
- Bitkom: „Umsetzungsleitfaden zur KI-Verordnung“ (01/2026)
- GDD-Kurzpapier „Mitbestimmungsrecht des Betriebsrats beim Einsatz von KI“ (06/2025)
- DSK „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ (06/2025)
- KI-Service-Desk der BNetzA
- AI-Act-Service-Desk der EU-Kommission

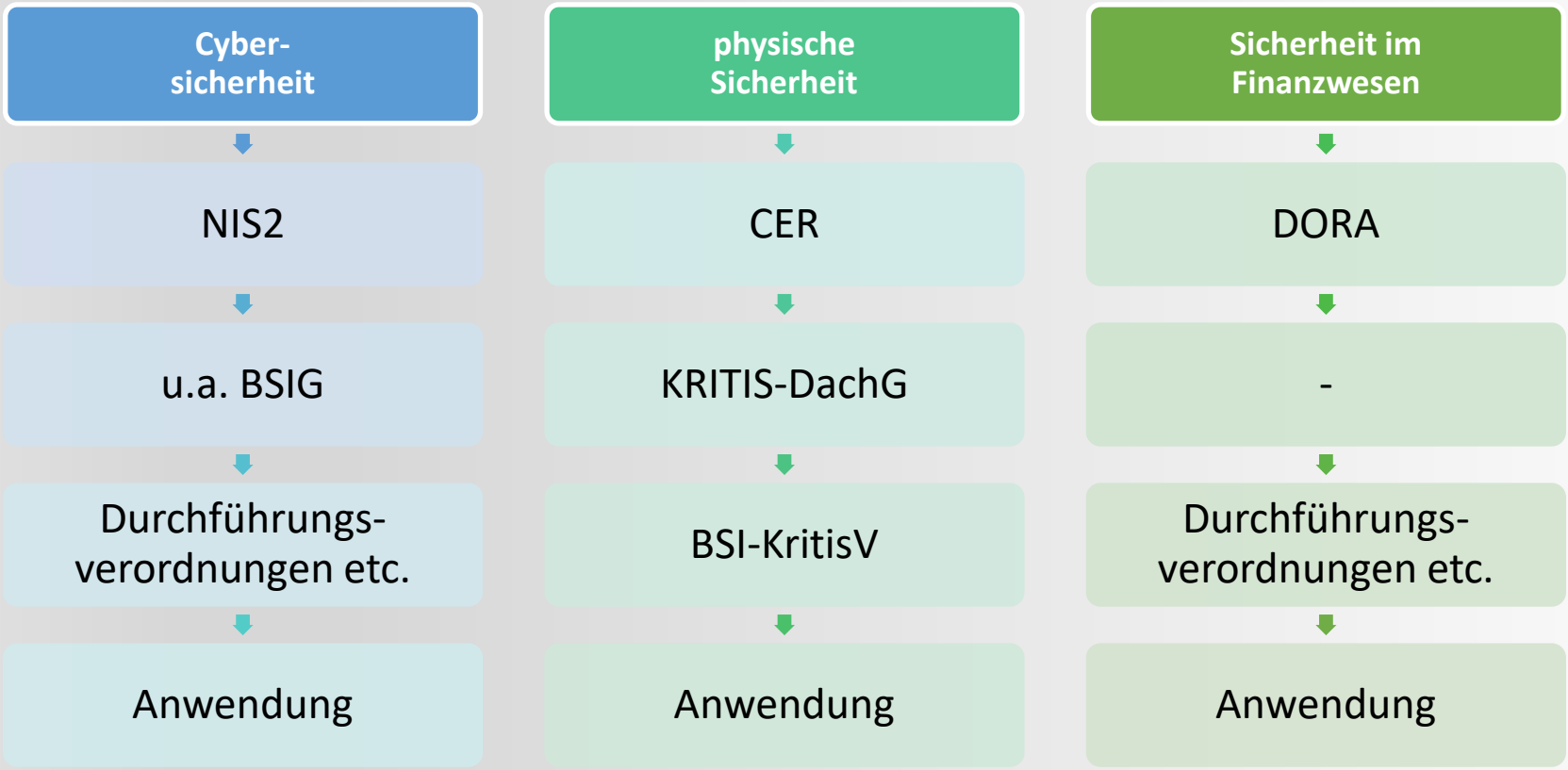
PRIVACYXPERTS

3

NIS2 / dt. Umsetzungsgesetz

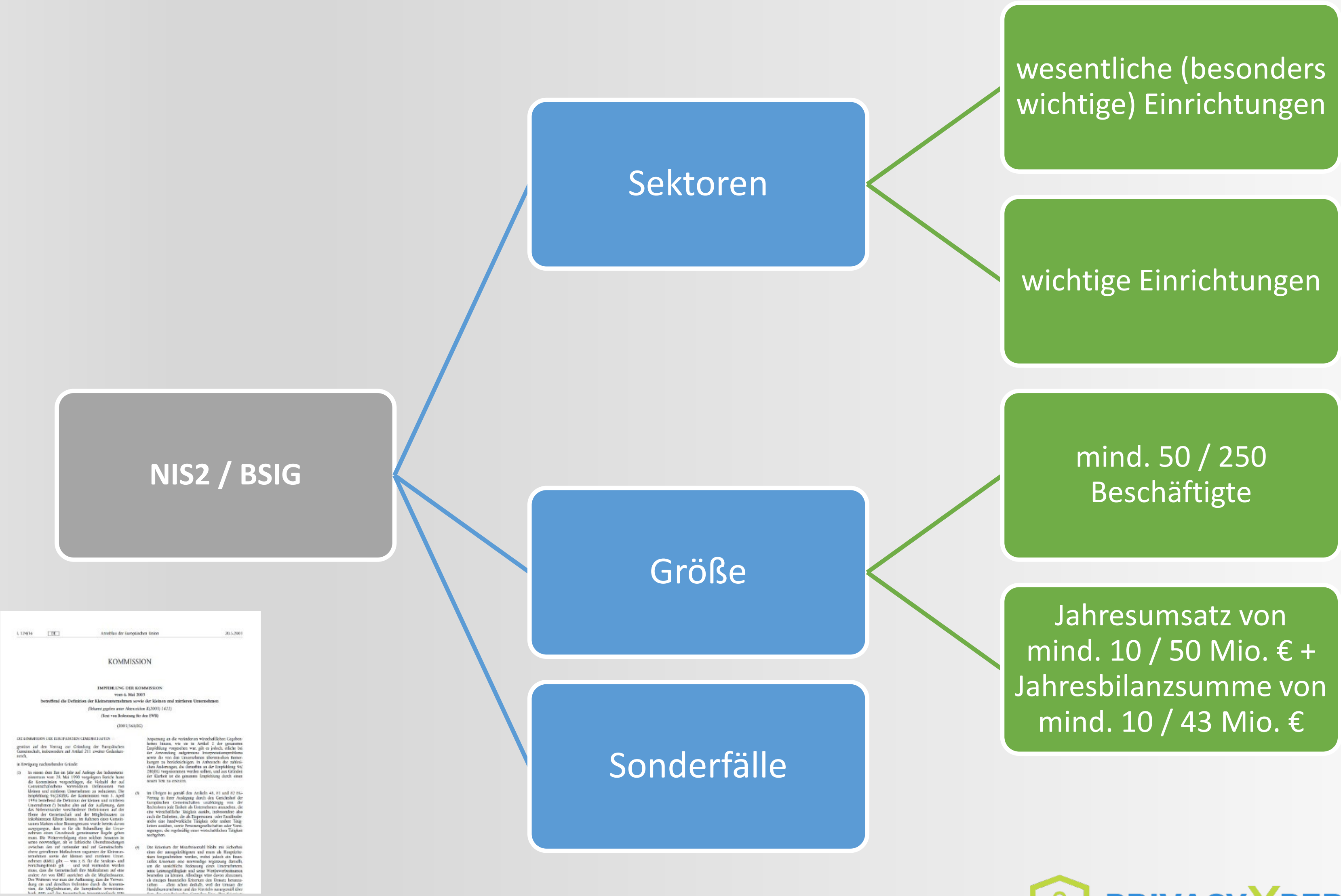
PRIVACY XPERTS

NIS2 / BSIG



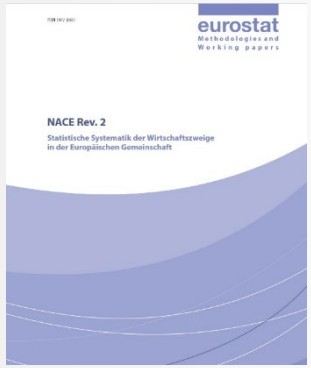
PRIVACYXPERTS

NIS2 / BSIG



Quelle: EU

NIS2 / BSIG



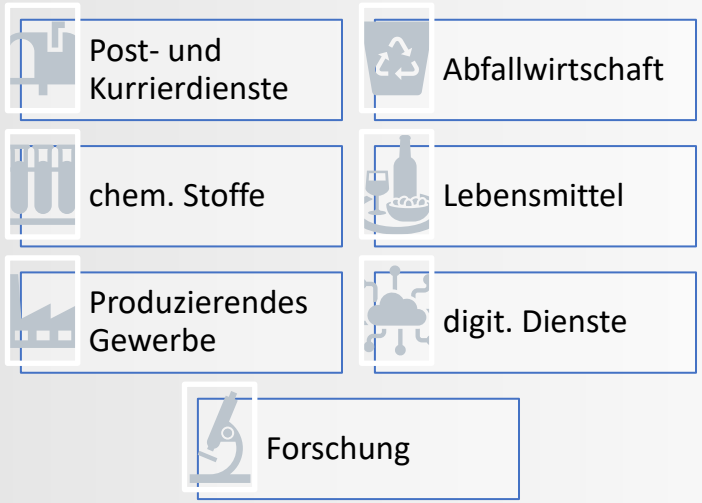
Quelle: EU

- **Art. 2, 3 NIS2**
  - Anhang I NIS2
    - Def. gem. Art. 6 NIS2
    - NACE Rev. 2
    - div. EU-VO & EU-RL
      - ggf. weitere EU-VO & EU-RL
  - Anhang II NIS2
    - Def. gem. Art. 6 NIS2
    - NACE Rev. 2
    - div. EU-VO & EU-RL
      - ggf. weitere EU-VO & EU-RL

PRIVACYXPERTS

NIS2 / BSIG

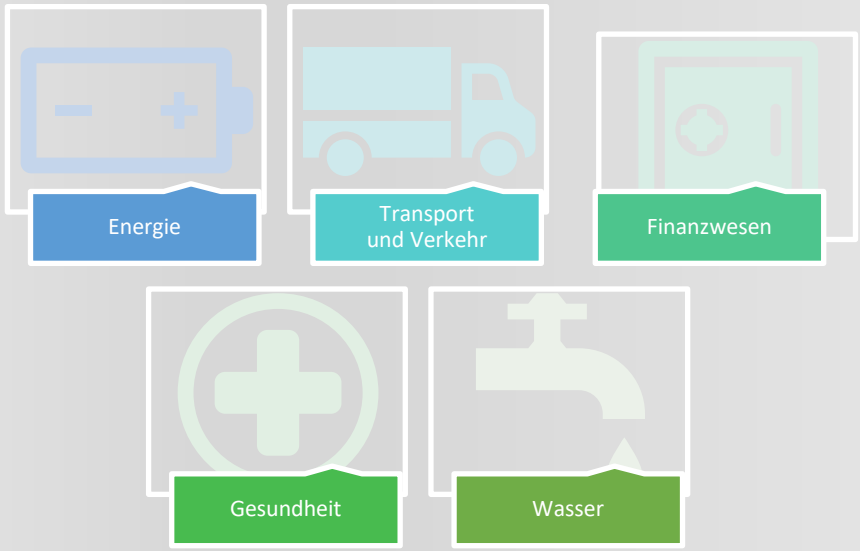
wesentliche Einrichtungen (Anhang I NIS2)



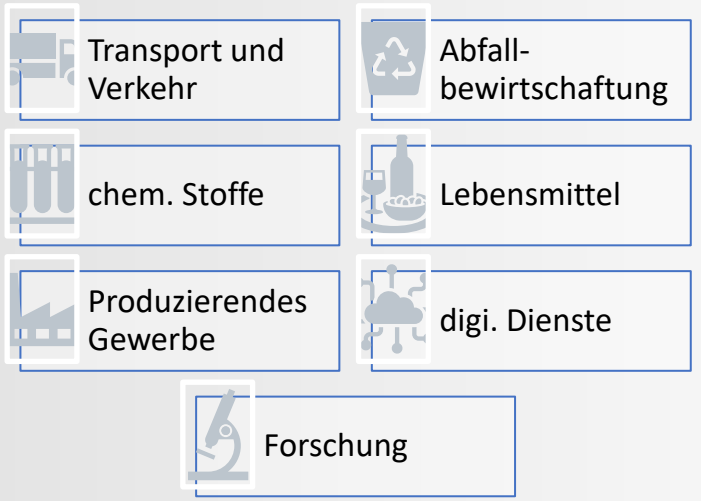
wichtige Einrichtungen (Anhang II NIS2)

PRIVACYXPERTS

NIS2 / BSIG



besonders wichtige Einrichtungen (Anlage 1 BSIG)



wichtige Einrichtungen (Anlage 2 BSIG)

PRIVACYXPERTS

NIS2 / BSIG

- **Pflichten („geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“, vgl. Art. 21 NIS2, § 30 BSIG)**
- **Konzepte** in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von **Sicherheitsvorfällen**
- **Aufrechterhaltung des Betriebs**, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- **Sicherheit der Lieferkette** einschließl. sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei **Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen**, einschließl. Management und Offenlegung von Schwachstellen
- **Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Cybersicherheit
- grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und ggf. **Verschlüsselung**
- **Sicherheit des Personals**, Konzepte für die Zugriffskontrolle und Management von Anlagen
- Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, **gesicherte Sprach-, Video- und Textkommunikation** sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

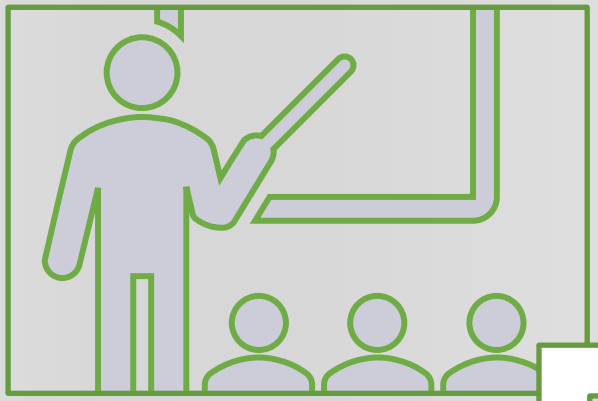
PRIVACYXPERTS

NIS2 / BSIG

- **Pflicht zur Meldung von erheblichen Sicherheitsvorfällen (vgl. Def. in Art. 6 Nr. 6, Art. 23 Abs. 3 NIS2)**
- **frühe Erstmeldung**: unverzüglich, spätestens innerhalb von 24 Std. nach Kenntniserlangung
- **bestätigende Erstmeldung**: unverzüglich, spätestens innerhalb von 72 Std. nach Kenntniserlangung
- ggf. **Zwischenmeldung** über Statusänderung (in Abstimmung mit dem BSI)
- **Abschlussmeldung**: spätestens einen Monat nach Übermittlung der bestätigenden Erstmeldung (u.a. mit ausführlicher Beschreibung des Vorfalls und Angaben zu Schweregrad und Auswirkungen, Art der Bedrohung bzw. Vorfallursache, Abhilfemaßnahmen, evtl. grenzüberschreitenden Auswirkungen

PRIVACYXPERTS

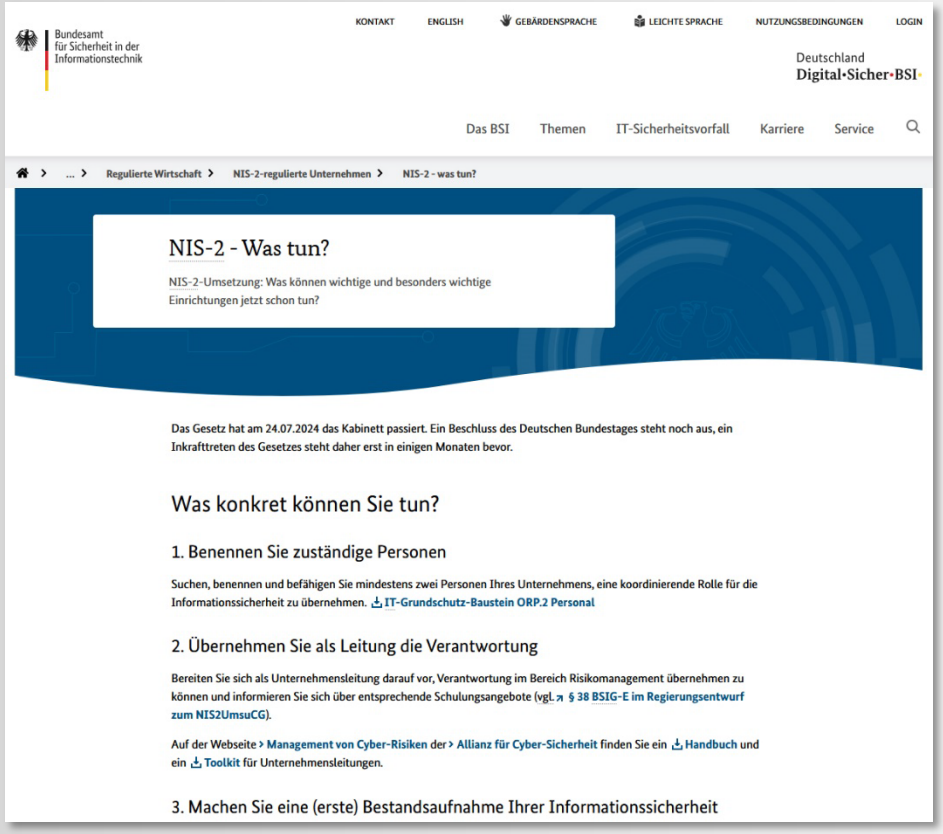
NIS2 / BSIG



*„Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden **Risikomanagement-maßnahmen umzusetzen** und ihre Umsetzung zu **überwachen**.“*
(§ 38 Abs. 1 BSIG)

PRIVACYXPERTS

NIS2 / BSIG



Quelle: #nis2know / BSI

4

Cyber Resilience Act

CRA

10. Dezember 2024

- Inkrafttreten

11. September 2026

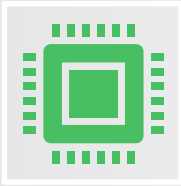
- Pflicht zur Meldung aktiv ausgenutzter Schwachstellen

11. September 2027

- Pflicht zur Erfüllung aller CRA-Pflichten

Produkte mit digit. Elementen

wichtige Produkte mit digit. Elementen – Klasse I



wichtige Produkte mit digit. Elementen – Klasse II

kritische Produkte mit digit. Elementen

PRIVACYXPERTS

CRA

Produkte mit digit. Elementen	wichtige Produkte mit digit. Elementen – Klasse I	wichtige Produkte mit digit. Elementen – Klasse II	kritische Produkte mit digit. Elementen
• Textverarbeitung • Tabellenkalkulation • Fotobearbeitung • Festplatten • … • *(ca. 90% aller erfassten Produkte)*	•Passwort-Manager •Netzmanagementsysteme •Bootmanager •Betriebssysteme •Router, Modems, Switches •smartes Spielzeug •virtuelle Assistenten für Smart Home •…	•Firewalls, Intrusion-Detection-Systeme, Intrusion-Prevention-Systeme •manipulationssichere Mikroprozessoren •manipulationssichere Mikrocontroller	•Hardwaregeräte mit Sicherheitsboxen •Smart-Meter-Gateways •Chipkarten •…

PRIVACYXPERTS

CRA

- **Grundlegende Cybersicherheitsanforderungen [1/2]**
- Bereitstellung auf dem Markt **ohne bekannte ausnutzbare Schwachstellen**
- Bereitstellung auf dem Markt mit einer **sicheren Standardkonfiguration**, sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digit. Elementen nichts anderes vereinbart wurde (und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen)
- Sicherstellen, dass **Schwachstellen durch Sicherheitsaktualisierungen behoben** werden können, ggf. auch durch automatische Sicherheitsaktualisierungen, die als Standardeinstellung innerhalb eines angemessenen Zeitrahmens installiert werden sowie über einen klaren und benutzerfreundlichen Opt-out-Mechanismus verfügen, bei dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können
- durch geeignete Kontrollmechanismen **Schutz vor unbefugtem Zugriff** bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden
- die **Vertraulichkeit** gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten **schützen**, z.B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel
- die **Integrität** gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung **schützen** und deren **Beschädigung melden**

PRIVACYXPERTS

CRA

- **Grundlegende Cybersicherheitsanforderungen [2/2]**
- die **Verarbeitung personenbezogener** oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digit. Elementen erforderliche Maß **beschränken** („Datenminimierung“)
- die **Verfügbarkeit** wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), **sicherstellen**
- die **negativen Auswirkungen** von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste **minimieren**
- so konzipiert, entwickelt und hergestellt werden, dass sie — auch bei externen Schnittstellen — **möglichst geringe Angriffsflächen** bieten
- so konzipiert, entwickelt und hergestellt werden, dass die **Auswirkungen eines Sicherheitsvorfalls** durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung **verringert** werden
- **sicherheitsbezogene Informationen** durch Aufzeichnung und / oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen und den Nutzern einen Opt-out-Mechanismus zur Verfügung stellen
- den Nutzern die Möglichkeit bieten, **alle Daten und Einstellungen dauerhaft sicher und einfach zu löschen**, und, wenn diese Daten auf andere Produkte oder Systeme übertragen werden können, sicherstellen, dass dies auf sichere Weise geschieht

PRIVACYXPERTS

5

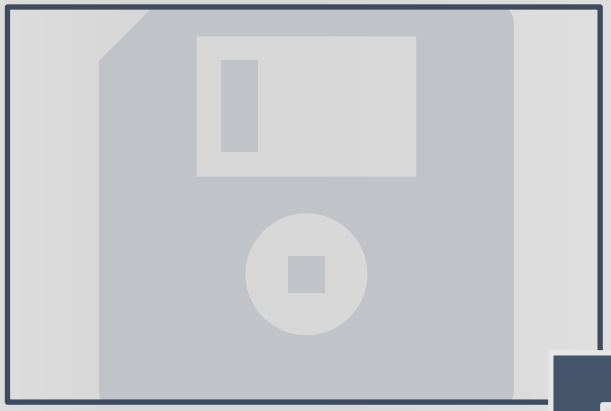
Data Act

DA

- **EU-Datenverordnung (sog. Data Act)**
- bereits in Kraft getreten; anzuwenden seit 12. September 2025
- enthält **nutzer- & produktbezogene** Vorschriften
- versch. Regelungsbereiche
  - Datenbereitstellung von Unternehmen an Privatpersonen oder an andere Unternehmen („**Data Sharing**“) (Art. 3-13 DA)
  - „**Cloud-Switching**“ (Art. 23-31 DA)
  - Datenüberlassung an **öffentl. Stellen** (Art. 14-22 DA)
- gilt im **B2C-, B2B- & B2G-Bereich**
- keine Rechtsgrundlage für Verarbeitung **personenbezogener Daten**
- zentraler Teil der **EU-Datenstrategie**

PRIVACYXPERTS

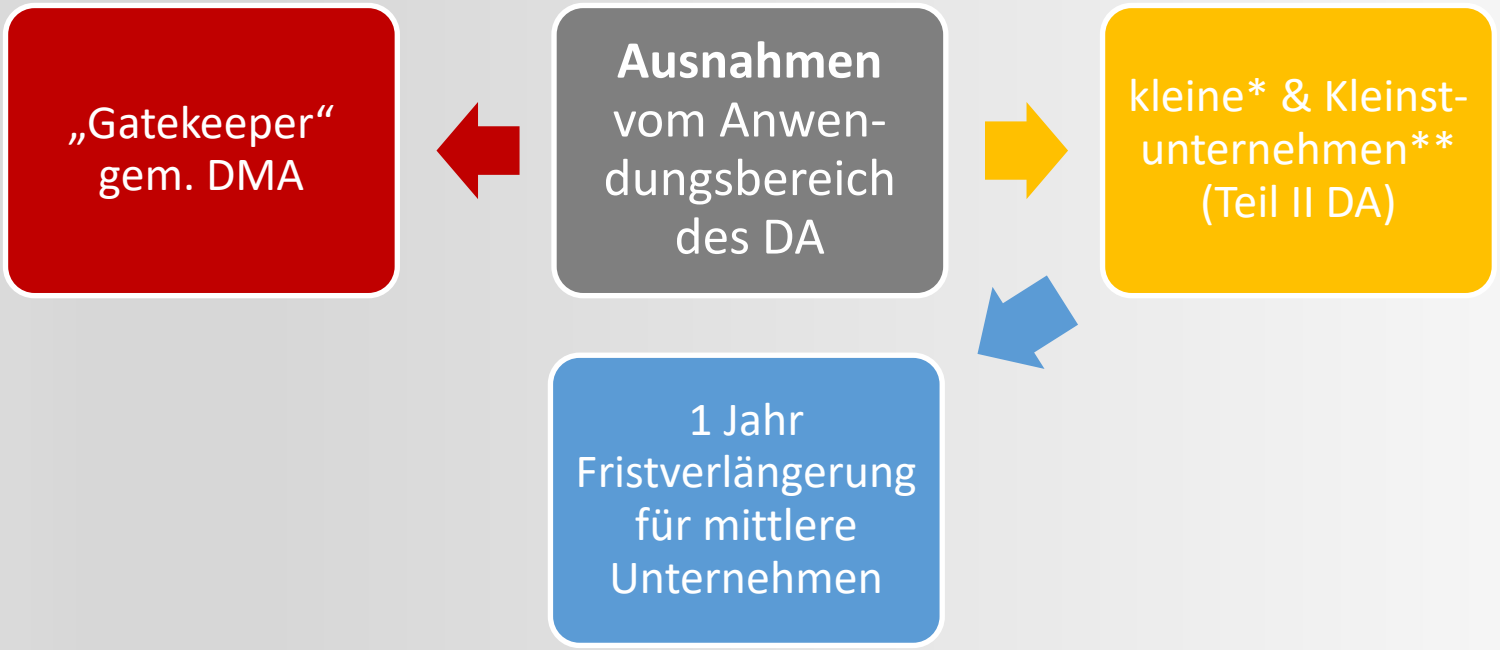
DA



*„Mit dieser Verordnung wird sichergestellt, dass die **Nutzer** eines vernetzten Produkts oder verbundenen Dienstes […] **auf die Daten zugreifen** können, die […] generiert werden, und dass diese Nutzer die **Daten verwenden** und auch an Dritte […] **weitergeben** können. Sie **verpflichtet Dateninhaber**, die Daten unter bestimmten Umständen den Nutzern und Dritten […] **bereitzustellen**.“ (ErwGr. 5 DA)*

PRIVACYXPERTS

DA



* kleine Unternehmen: weniger als 50 MA und weniger als 10 Mio. € Umsatz oder Bilanzsumme
** Kleinstunternehmen: weniger als 10 MA und weniger als 2 Mio. € Umsatz oder Bilanzsumme

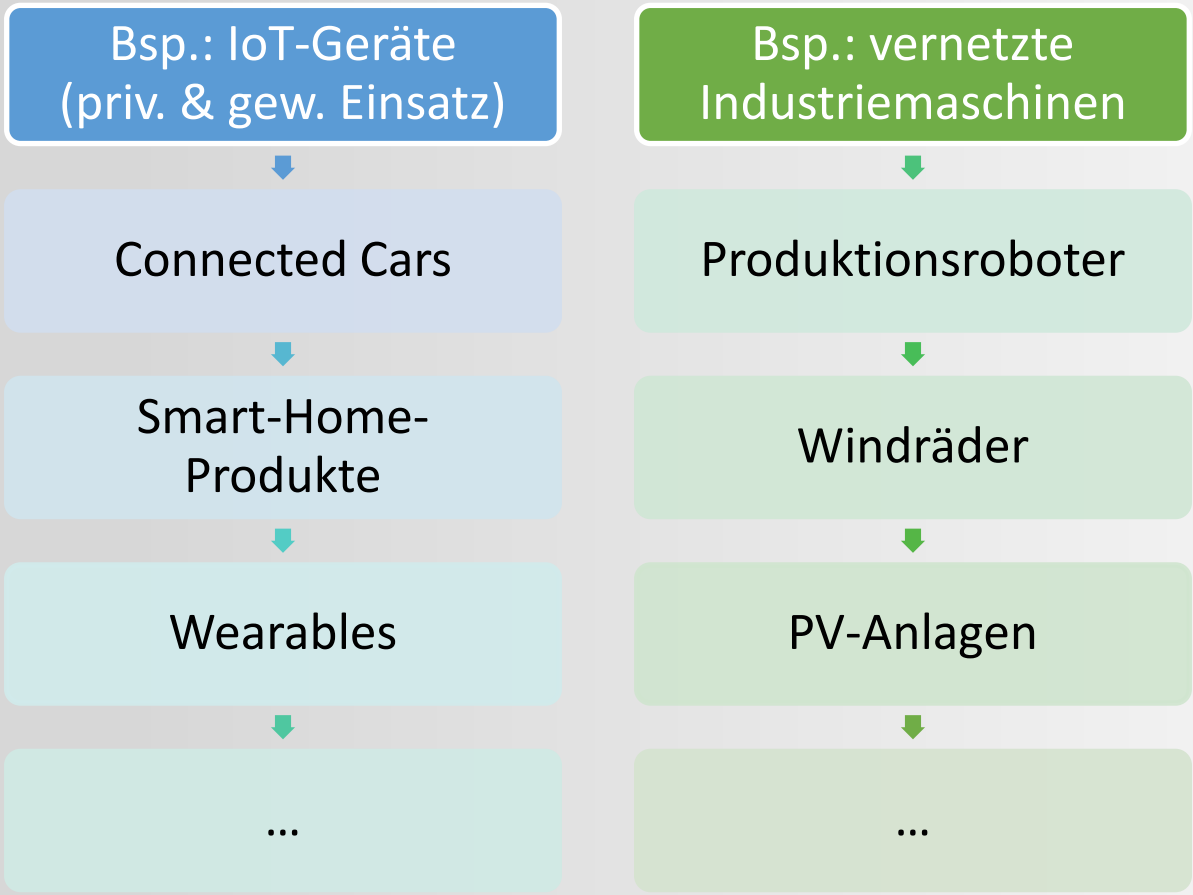
PRIVACYXPERTS

DA

- **ErwGr. 14 DA**
- *"Vernetzte Produkte kommen in allen Bereichen der Wirtschaft und Gesellschaft vor, einschließlich in privaten, zivilen oder gewerblichen **Infrastrukturen**, **Fahrzeugen**, **medizinischer Ausrüstung**, **Lifestyle-Ausrüstung**, **Schiffen**, **Luftfahrzeugen**, **Haushaltsgeräten** und **Konsumgütern**, **Medizin- und Gesundheitsprodukten** oder **landwirtschaftlichen und industriellen Maschinen und Anlagen**."*

PRIVACY XPERTS

DA



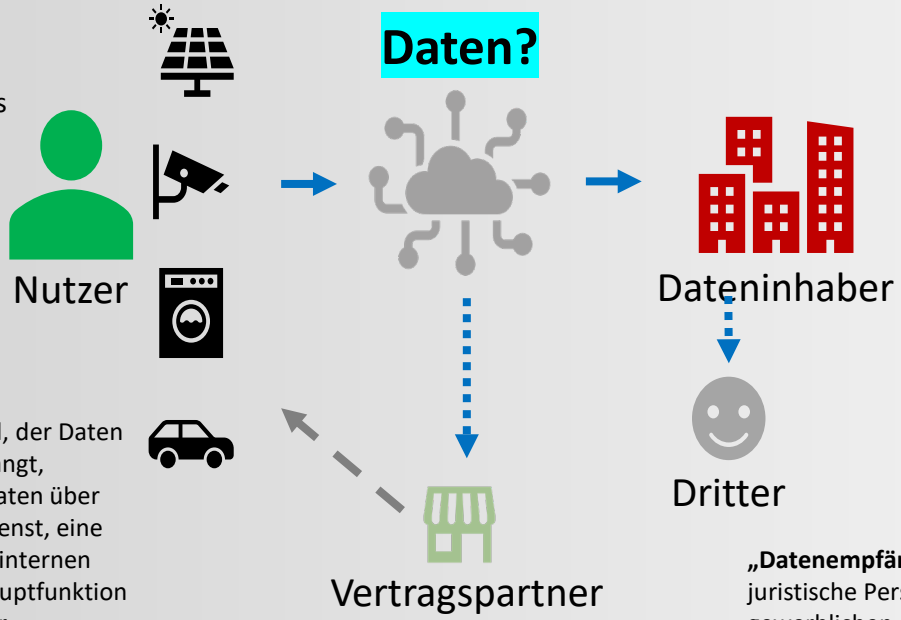
inkl. virtueller Assistenten, wie Siri, Alexa & Co. (Art. 1 Abs. 4, 2 Nr. 31 DA)

ausgenommen sind u.a. **Server- oder Cloud-Infrastrukturen** (Art. 2 Nr. 5 DA)

PRIVACYXPERTS

DA

„Nutzer“ ist eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt



„Dateninhaber“ ist eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat

„vernetztes Produkt“ ist ein Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist

„verbundener Dienst“ ist ein digitalen Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen

„Datenempfänger“ ist eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, Daten bereitstellt

PRIVACYXPERTS

DA

- **Daten (digitalisierte Nutzungshandlungen)**
- **„Daten“**: jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material (Art. 2 Nr. 1 DA)
- **„Produktdaten“**: Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können (Art. 2 Nr. 15 DA)
- **„verbundene Dienstdaten“**: Daten, die die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden (Art. 2 Nr. 16 DA)
- **„ohne Weiteres verfügbare Daten“**: Produktdaten und verbundene Dienstdaten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, wobei über eine einfache Bearbeitung hinausgegangen wird (Art. 2 Nr. 17 DA)

PRIVACYXPERTS

DA

Pflicht zur Datenbereitstellung* (Art. 4 Abs. 1 DA)

***** ab dem 12. September 2025***

„ohne Weiteres verfügbare Daten“ & Meta-Daten

Zugang für Nutzer:

- unverzüglich
- einfach
- sicher
- unentgeltlich
- kontinuierlich
- ggf. in Echtzeit
- in gleicher Qualität wie für den Dateninhaber

Datenformat:

- umfassend
- gängig
- maschinenlesbar

PRIVACYXPERTS

DA

Data-Access-by-Design* (Art. 3 Abs. 1 DA)

Produkt-, Dienst- & Meta-Daten

Zugang für Nutzer:

- standardmäßig
- einfach
- sicher
- unentgeltlich
- ggf. direkt

Datenformat:

- umfassend
- strukturiert
- gängig
- maschinenlesbar

* ***Designpflicht*** *für alle Produkte und verbundene Dienste, die* ***ab dem 12. September 2026*** *in Verkehr gebracht werden (Art. 50 DA)*

PRIVACYXPERTS

DA

Pflichtinformationen

...zum vernetzten Produkt

...zum verbundenen Dienst

...zum Anbieterwechsel

...über einen intern. Datentransfer

...über ein evtl. Entgelt

EU Data Act

Der EU Data Act (Verordnung (EU) 2023/2854) ist ein zentrales Gesetzeswerk, das den Zugang zu und die Nutzung von Daten in der Europäischen Union regelt. Ziel ist es, faire und transparente Praktiken beim Datenaustausch sicherzustellen und sowohl Privatpersonen als auch Unternehmen zu befähigen, Zugriff auf die von vernetzten Geräten – einschließlich Fahrzeugen – generierten Daten zu erhalten und diese zu kontrollieren. Die Volkswagen AG verpflichtet sich zur Umsetzung von Lösungen, die den Anforderungen des EU Data Acts entsprechen, um Vertrauen in datengestützte Dienste und Innovationen zu stärken.

Weitere Informationen zum EU Data Act finden Sie unter folgendem Link:

Zur EU-Gesetzgebung

Ihre Daten, Ihre Rechte

Gemäß des EU Data Acts wahren wir die Prinzipien von Transparenz, Fairness und Nutzerkontrolle beim Datenaustausch. Die Verordnung stellt sicher, dass generierte Daten unter klar definierten Bedingungen zugänglich sind – unter Einhaltung höchster Sicherheits- und Datenschutzstandards.

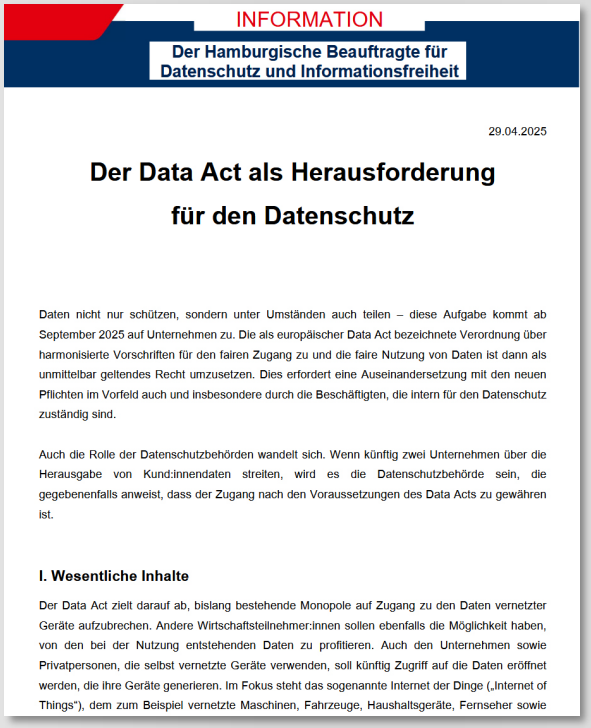
Zentrale Aspekte des EU Data Acts:

- Nutzerkontrolle & Transparenz: Privatpersonen und Unternehmen haben das Recht, auf ihre generierten Daten zuzugreifen und diese zu verwalten
- Fairer Zugang & Nutzung: Nutzer können ihre Daten selbst abrufen oder sicher mit ausgewählten Drittparteien teilen
- Datensicherheit & Rechtskonformität: Der Datenaustausch erfolgt unter strengen Sicherheitsvorkehrungen und gesetzlichen Rahmenbedingungen
- Mechanismen zur Streitbeilegung: Klare Verfahren regeln die Lösung von Konflikten beim Datenzugriff

Quelle: VW

PRIVACYXPERTS

DA



INFORMATION

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

29.04.2025

Der Data Act als Herausforderung für den Datenschutz

Daten nicht nur schützen, sondern unter Umständen auch teilen – diese Aufgabe kommt ab September 2025 auf Unternehmen zu. Die als europäischer Data Act bezeichnete Verordnung über harmonisierte Vorschriften für den fairen Zugang zu und die faire Nutzung von Daten ist dann als unmittelbar geltendes Recht umzusetzen. Dies erfordert eine Auseinandersetzung mit den neuen Pflichten im Vorfeld auch und insbesondere durch die Beschäftigten, die intern für den Datenschutz zuständig sind.

Auch die Rolle der Datenschutzbehörden wandelt sich. Wenn künftig zwei Unternehmen über die Herausgabe von Kund:innendaten streiten, wird es die Datenschutzbehörde sein, die gegebenenfalls anweist, dass der Zugang nach den Voraussetzungen des Data Acts zu gewähren ist.

I. Wesentliche Inhalte

Der Data Act zielt darauf ab, bislang bestehende Monopole auf Zugang zu den Daten vernetzter Geräte aufzubrechen. Andere Wirtschaftsteilnehmer:innen sollen ebenfalls die Möglichkeit haben, von den bei der Nutzung entstehenden Daten zu profitieren. Auch den Unternehmen sowie Privatpersonen, die selbst vernetzte Geräte verwenden, soll künftig Zugriff auf die Daten eröffnet werden, die ihre Geräte generieren. Im Fokus steht das sogenannte Internet der Dinge („Internet of Things"), dem zum Beispiel vernetzte Maschinen, Fahrzeuge, Haushaltsgeräte, Fernseher sowie

Europäische Kommission

DE Search

Gestaltung der digitalen Zukunft Europas

Home | Politikbereiche | Aktivitäten | Nachrichten | Bibliothek | Finanzierung | Kalender | Konsultationen | AI Office

Home > Fact Pages > Datengesetz erklärt

Datengesetz erklärt

Information notification

Dies ist eine maschinelle Übersetzung durch den eTranslation-Dienst der Europäischen Kommission, der Ihnen hilft, diese Seite zu verstehen. Bitte lesen Sie die Nutzungsbedingungen
Um die Originalfassung zu lesen, gehen Sie zur Quellenseite.

Ein umfassender Überblick über das Datengesetz, einschließlich seiner Ziele und seiner Funktionsweise in der Praxis.

Als PDF ausdrucken

Teilen

Warum das Datengesetz?

Das Datengesetz ist ein Gesetz zur Stärkung der Datenwirtschaft der EU und zur Förderung eines wettbewerbsfähigen Datenmarkts, indem Daten (insbesondere Industriedaten) leichter zugänglich und nutzbar gemacht werden, datengesteuerte Innovationen gefördert werden und die Datenverfügbarkeit erhöht wird. Um dies zu erreichen, sorgt das Datengesetz für eine faire Verteilung des Datenwerts unter den Akteuren der Datenwirtschaft. Sie verdeutlicht, *wer welche* Daten unter *welchen* Bedingungen verwenden darf. Nähere Informationen finden Sie in den häufig gestellten Fragen zum Datengesetz.

In den letzten Jahren hat die Verfügbarkeit von mit dem Internet verbundenen Produkten („verbundene Produkte") auf dem europäischen Markt rapide zugenommen. Diese Produkte, die zusammen ein Netzwerk bilden, das als Internet der Dinge (IoT) bekannt ist, erhöhen das Datenvolumen, das in der EU zur Wiederverwendung zur Verfügung steht, erheblich. Dies birgt ein enormes Potenzial für Innovation und Wettbewerbsfähigkeit in der EU.

Das Datengesetz gibt Nutzern vernetzter Produkte (Unternehmen oder Einzelpersonen, die ein solches Produkt besitzen, leasen oder mieten) eine größere Kontrolle über die von ihnen generierten Daten, während Anreize für diejenigen, die in Datentechnologien investieren, erhalten bleiben. Darüber hinaus werden allgemeine Bedingungen für Situationen festgelegt, in denen ein Unternehmen gesetzlich verpflichtet ist, Daten an ein anderes Unternehmen weiterzugeben.

Europäische Kommission

DE Search

Gestaltung der digitalen Zukunft Europas

Home | Politikbereiche | Aktivitäten | Nachrichten | Bibliothek | Finanzierung | Kalender | Konsultationen | AI Office

Home > Bibliothek > Kommission veröffentlicht häufig gestellte Fragen zum Datengesetz

POLICY AND LEGISLATION | Veröffentlichung 06 September 2024

Kommission veröffentlicht häufig gestellte Fragen zum Datengesetz

Information notification

Dies ist eine maschinelle Übersetzung durch den eTranslation-Dienst der Europäischen Kommission, der Ihnen hilft, diese Seite zu verstehen. Bitte lesen Sie die Nutzungsbedingungen
Um die Originalfassung zu lesen, gehen Sie zur Quellenseite.

Die häufig gestellten Fragen (FAQs) zum Datengesetz werden seine Umsetzung unterstützen.

Mit dem Datengesetz wird ein horizontales Regelwerk für den Datenzugang und die Datennutzung festgelegt, das den Schutz der Grundrechte achtet und weitreichende Vorteile für die europäische Wirtschaft und Gesellschaft bietet. Sie erhöht die Verfügbarkeit von Daten – insbesondere von Industriedaten – und fördert datengesteuerte Innovationen bei gleichzeitiger Gewährleistung einer fairen Verteilung des Datenwerts auf alle Akteure der Datenwirtschaft. Eine Einführung in das Datengesetz finden Sie auf der Faktenseite „Datengesetz erläutert".

Das Datengesetz tritt am 12. September 2025 in Kraft. Zusammen mit dem Daten-Governance-Gesetz, das das Vertrauen in freiwillige Mechanismen für den Datenaustausch stärkt, wird das Datengesetz zur Schaffung eines echten Binnenmarkts für Daten beitragen und Europa zu einem Vorreiter in der globalen Datenwirtschaft machen.

Nachfolgend können Sie die PDF-Version der FAQs zum Datengesetz herunterladen. Dieses Dokument wurde mit Beiträgen verschiedener Interessenträger erstellt und wird die Umsetzung des Datengesetzes unterstützen.

iStock Getty Images+ 1297151834 © metamorworks

Zugehörige Themen

Big Data | Datennichtlinie | Offene Daten

Downloads

FAQs Data Act — Herunterladen

„Umsetzungsleitfaden zum Data Act" (Bitkom)

Quellen:

HBfDI: „Handreichung zum Data Act"

EU: „Datengesetz erklärt" / „FAQ zum Data Act"

PRIVACYXPERTS

6

Geschäftsgeheimnisgesetz

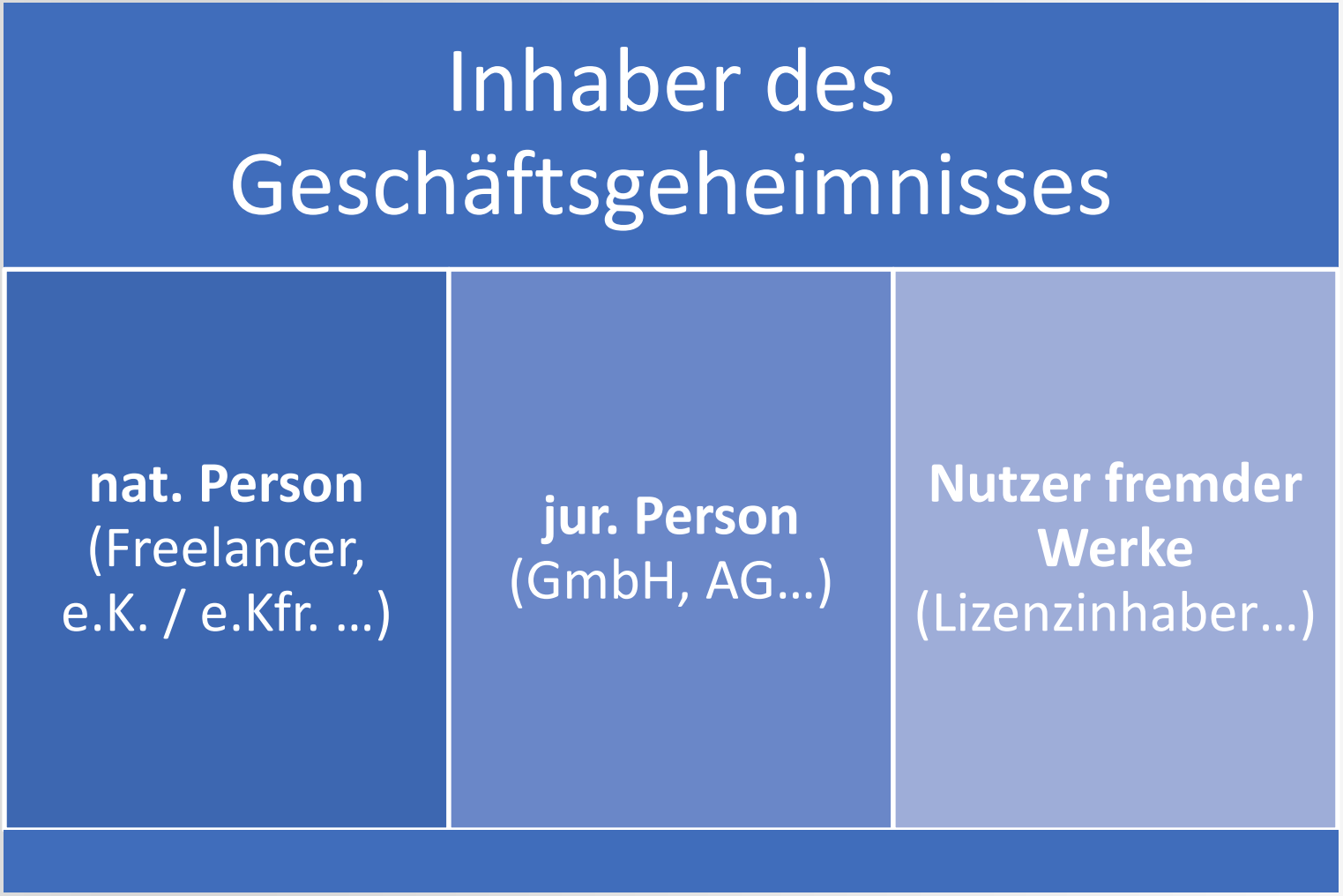
GeschGehG

PRIVACYXPERTS

GeschGehG

PRIVACYXPERTS

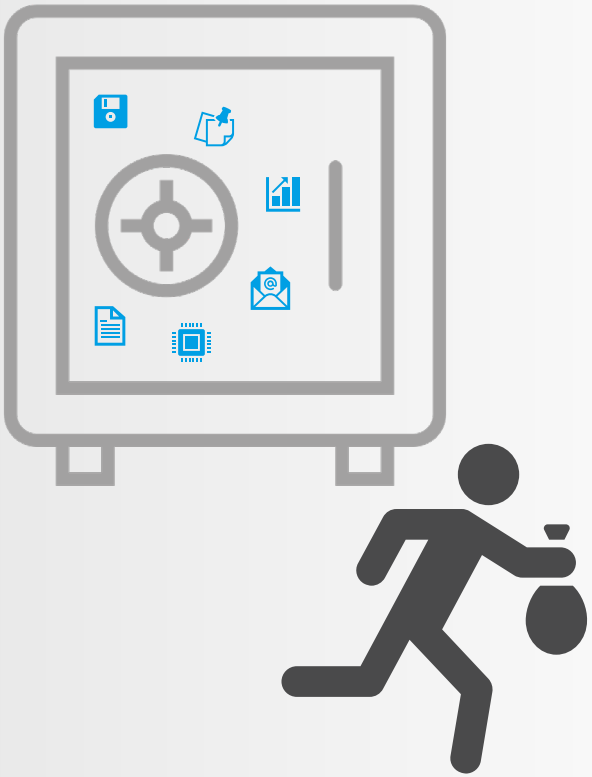
GeschGehG



PRIVACYXPERTS

GeschGehG

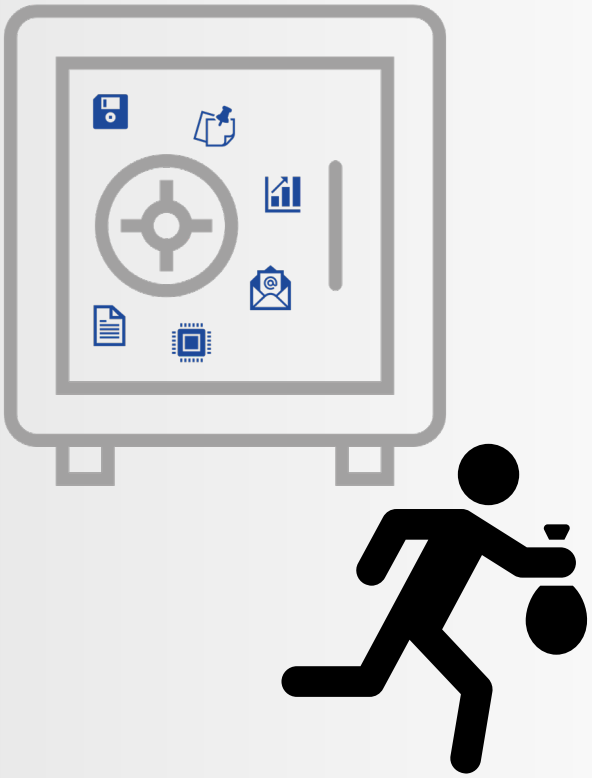
- **§ 4 Abs. 1 GeschGehG:** Ein Geschäftsgeheimnis darf nicht erlangt werden durch…
- unbefugten **Zugang** zu, unbefugte **Aneignung** oder unbefugtes **Kopieren** von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der **rechtmäßigen Kontrolle** des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis **enthalten** oder aus denen sich das Geschäftsgeheimnis **ableiten lässt**, oder
- jedes **sonstige Verhalten**, das unter den jeweiligen Umständen nicht dem **Grundsatz von Treu und Glauben** unter Berücksichtigung der anständigen **Marktgepflogenheit** entspricht



PRIVACYXPERTS

GeschGehG

- **§ 4 Abs. 3 GeschGehG:** Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer…
- es **über eine andere Person erlangt** hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung **weiß oder wissen müsste**, dass diese das Geschäftsgeheimnis **unberechtigt genutzt oder offengelegt** hat
- (gilt insbesondere, wenn die Nutzung in der **Herstellung**, dem **Anbieten**, dem **Inverkehrbringen** oder der **Einfuhr**, der **Ausfuhr** oder der **Lagerung** für diese Zwecke von **rechtsverletzenden Produkten** besteht)



PRIVACYXPERTS

GeschGehG

- **§ 3 Abs. 1 GeschGehG:** Ein Geschäftsgeheimnis darf insbesondere erlangt werden durch…
- eine **eigenständige Entdeckung oder Schöpfung**;
- ein **Beobachten, Untersuchen, Rückbauen oder Testen** eines Produkts oder Gegenstands, das oder der
  a) **öffentlich verfügbar** gemacht wurde oder
  b) sich im **rechtmäßigen Besitz** des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur **Beschränkung der Erlangung des Geschäftsgeheimnisses** unterliegt;
- ein **Ausüben von Informations- und Anhörungsrechten der Arbeitnehmer** oder Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretung

PRIVACYXPERTS

GeschGehG

erlaubte Nutzung eines Geschäftsgeheimnisses

vertraglich

gesetzlich

PRIVACYXPERTS

GeschGehG

- **Sanktionen**
- Anspruch auf **Auskunft** bzw. Schadenersatz bei verspäteter oder nicht erteilter Auskunft (§ 8 GeschGehG)
- Anspruch auf **Schadenersatz** (§ 10 GeschGehG)
- ggf. Anspruch ggü. **Arbeitgeber des Rechtsverletzers** (§ 12 GeschGehG)

PRIVACYXPERTS

NIS2

Merke:

Im Zweifel immer einen risikobasiertem Ansatz verfolgen: je höher das Risiko, desto mehr muss getan werden, um zu verhindern, dass es eintritt!

Vielen Dank für Ihre Aufmerksamkeit!

Gibt es noch Fragen?

Ihr Referent:

Rechtsanwalt
Michael Rohrlich

PRIVACYXPERTS