Niederrhein Protected 2025

IT-Sicherheit für den Mittelstand

Cybersicherheit zwischen rechtlicher Pflicht und rechtlichen Grenzen

Duisburg, 25.02.2025

Dr. Jens Eckhardt
Rechtsanwalt und Fachanwalt für IT-Recht
Datenschutz-Auditor (TÜV)
IT-Compliance Manager (TÜV)

1

Agenda

- **Von der Richtlinie zur Umsetzung**
- Wer ist betroffen?
- Pflichten für § 28-Unternehmen
- Exkurs: Verhältnis zur DS-GVO
- Fragen und Diskussion

2

NIS-2-Umsetzung: Von der Richtlinie zur Umsetzung

- **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf**
  - **Grund:** NIS-2 Richtlinie (Richtlinie (EU) 2022/2555 vom 14.12.2022)
    (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (Stand: 23.02.2025))
    - **Inkrafttreten:** 16. Januar 2023 – **Umsetzungsfrist bis:** 17. Oktober 2024
    - Keine vertikale Direktwirkung – Erforderlichkeit eines Umsetzungsgesetzes
  - **Inkrafttreten:** voraussichtlich Herbst 2025, aber tatsächlich unklar
    - NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-**Regierungs**entwurf **vom 02.10.2024**
      (https://dserver.bundestag.de/btd/20/131/2013184.pdf (Stand des Links: 23.02.2025))
  - **„Artikel-Gesetz" mit 30 Artikeln**
    - Schwerpunkt: BSI-Gesetz-RegE
    - diverse „Folgeänderungen" in Gesetzen (u.a. TDDDG)
    - **Inkrafttreten: Tag nach der Verkündung (Art. 33)**
  - **Umsetzungsfrist nach BSIG: KEINE**, aber bestimmte Pflichten mit Fristen
    - Registrierungspflicht (§ 33 BSIG-RegE): binnen 3 Monaten
    - Nachweispflicht der Maßnahme bei kritischen Anlagen (§ 39 BSIG-RegE): Einzelfallfestlegung durch BSI, aber 3 Jahre

3

NIS-2-Umsetzung: Von der Richtlinie zur Umsetzung

- **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf**
  - **Grund:** NIS-2 Richtlinie (Richtlinie (EU) 2022/2555 vom 14.12.2022)
    (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (Stand: 23.02.2025))
    - **Inkrafttreten:** 16. Januar 2023 – **Umsetzungsfrist bis:** 17. Oktober 2024
    - Keine vertikale Direktwirkung – Erforderlichkeit eines Umsetzungsgesetzes
  - **Inkrafttreten:** voraussichtlich Herbst 2025, aber tatsächlich unklar
    - NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-**Regierungs**entwurf **vom 02.10.2024**
      (https://dserver.bundestag.de/btd/20/131/2013184.pdf (Stand des Links: 23.02.2025))
  - **„Artikel-Gesetz" mit 30 Artikeln**
    - Schwerpunkt: BSI-Gesetz-RegE
    - diverse „Folgeänderungen" in Gesetzen (u.a. TDDDG)
    - **Inkrafttreten: Tag nach der Verkündung (Art. 33)**
  - **Umsetzungsfrist nach BSIG: KEINE**, aber bestimmte Pflichten mit Fristen
    - Registrierungspflicht (§ 33 BSIG-RegE): binnen 3 Monaten
    - Nachweispflicht der Maßnahme bei kritischen Anlagen (§ 39 BSIG-RegE): Einzelfallfestlegung durch BSI, aber 3 Jahre

4

NIS-2-Umsetzung: Von der Richtlinie zur Umsetzung *- EXKURS -*

- **BSIG-Regierungsentwurf**
  - Teil 1 (§§ 1 – 2) Allgemeine Vorschriften (Begriffsbestimmungen in § 2)
  - Teil 2 (§§ 3 – 27) Das Bundesamt
  - **Teil 3 (§§ 28 – 48 Sicherheit in der Informationstechnik von Einrichtungen**
    - **Kapitel 1 Anwendungsbereich (§§ 28, 29)**
    - **Kapitel 2 Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten (§§ 30 - 42)**
    - **Kapitel 3 Informationssicherheit der Einrichtungen der Bundesverwaltung (§§ 43 – 48)**
  - Teil 4 (§§ 49 – 51) Datenbanken der Domain-Name-Registrierungsdaten
  - Teil 5 (§§ 51 – 55) Zertifizierung, Konformitätserklärung und Kennzeichen
  - Teil 6 (§§ 56 – 58)Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten
  - Teil 7 (§§ 59 - 64) Aufsicht
  - Teil 8 (§ 65) Bußgeldvorschriften
  - **Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen**
  - **Anlage 2 Sektoren wichtiger Einrichtungen**

Agenda

- Von der Richtlinie zur Umsetzung
- **Wer ist betroffen?**
- Pflichten für § 28-Unternehmen
- Exkurs: Verhältnis zur DS-GVO
- Fragen und Diskussion

NIS-2-Umsetzung: Wer ist betroffen?

- **Unmittelbar Betroffene des BSIG-RegE**
  - **Besonders wichtige und wichtige Einrichtungen**
    - **besonders wichtige Einrichtungen** („*essential entities*“) (§ 28 Abs. 1)
    - **wichtige Einrichtungen** („*important entities*“) (§ 28 Abs. 2)
    - Ausnahmen von einzelnen Regelungen für bestimmte Unternehmen (Abs. 4, 5)
    - Ausnahmen für best. Anbieter von Leistungen an Bundesverwaltung (Abs. 9)
    - Pflichten nach §§ 30 bis 42 BSIG-RegE
    - Unterscheidung (nur) in Bezug auf Bußgeldhöhe nach § 67 Abs. 6, 7 BSIG-RegE und Aufsichts- und Durchsetzungsmaßnahmen (§§ 64, 65 BSIG-RegE)
  - **Betreiber kritischer Anlagen** = Unterfall der besonders wichtigen Einrichtungen
  - **Einrichtungen der Bundesverwaltung** (§ 29)
    - § 28 Abs. 1 S. 2 und Abs. 2 S. 2: Nicht erfasst durch § 28, „*sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind*“
    - Pflichten nach §§ 43 – 50 BSIG-RegE
- **Mittelbar betroffene Unternehmen: Zulieferer, Supply-Chain, Auftragnehmer und Unterauftragnehmer**
  - **proaktive oder reaktive Umsetzung**
  - **„NIS-Sicherheitsvereinbarung“?: Wer gibt die Inhalte vor?**

7

NIS-2-Umsetzung: Wer ist betroffen?
- EXKURS zum Nachlesen -

- **„besonders wichtige Einrichtungen“** (§ 28 Abs. 1 BSIG-RegE) („*essential entities*“)
  - **Betreiber kritischer Anlagen** (Definition in § 28 Abs. 7 i.V.m. § 2 Nr. 22, § 56 Abs. 4 BSIG-RegE)
  - **qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter**
  - Anbieter **öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze**, die a) mindestens 50 Mitarbeiter beschäftigen oder b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen
  - Sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer **der in Anlage 1 bestimmten Einrichtungsarten** zuzuordnen sind **und** die a) **mindestens 250 Mitarbeiter** beschäftigen **oder** b) einen **Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro** aufweisen

- **„wichtige Einrichtungen“** (§ 28 Abs. 2 BSIG-RegE) („*important entities*“)
  - **Vertrauensdiensteanbieter** → Art. 3 Nr. 19 Verordnung (EU) Nr. 910/2014 (eIDAS-VO)
  - **Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze**, die a) weniger als 50 Mitarbeiter beschäftigten und b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen
  - natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in **Anlagen 1 und 2 bestimmten Einrichtungsarten** zuzuordnen sind **und** die a) **mindestens 50 Mitarbeiter** beschäftigen **oder** b) einen **Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro** aufweisen

8

NIS-2-Umsetzung: Wer ist betroffen?
- EXKURS zum Nachlesen -

- **Berechnungsmodalität (§ 28 Abs. 3 BSIG-RegE)**

  „Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist ***auf*** *1.* ***die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen*** *und 2. außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.*

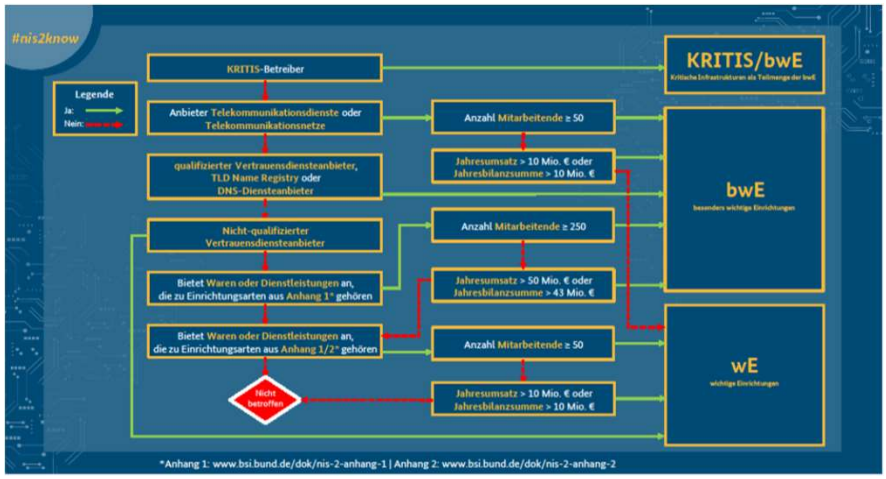
  Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzuzurechnen, wenn *das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, unabhängig von seinen Partner- oder verbundenen Unternehmen ist.“*

- **Sektoren der Kritischen Anlagen nach § 28 Abs. 7 BSIG-RegE**
  - Energie
  - Transport und Verkehr
  - Finanz- und Versicherungswesen
  - Gesundheitswesen
  - Wasser
  - Ernährung
  - Informationstechnik und Telekommunikation
  - Weltraum
  - Siedlungsabfallentsorgung

- **Sektoren der Einrichtungen nach § 28 Abs. 1 und 2 i.V.m. Anlage 1 und 2 BSIG-RegE**
  - Energie
  - Transport und Verkehr
  - Finanz- und Versicherungswesen
  - Gesundheitswesen
  - Wasser
  - Ernährung
  - Informationstechnik und Telekommunikation
  - Weltraum
  - Abfallbewirtschaftung
  - Produktion, Herstellung und Handel mit chemischen Stoffen
  - Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe/ Herstellung von Waren (bestimmte Branchen)
  - Anbieter digitaler Dienste (Online-Marktplätze, Suchmaschinen, Soziale Netzwerke)
  - Forschung

9

NIS-2-Umsetzung: Entscheidungsbaum des BSI
- EXKURS zum Nachlesen -



QUELLE: **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.pdf?__blob=publicationFile&v=9 (Link mit Stand: 23.02.2025))**

10

Agenda

- Von der Richtlinie zur Umsetzung
- Wer ist betroffen?
- **Pflichten für § 28-Unternehmen**
- Exkurs: Verhältnis zur DS-GVO
- Fragen und Diskussion

11

NIS-2-Umsetzung: Pflichten für § 28-Unternehmen

- **Pflichten für „§ 28-Unternehmen“: Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten (Kapitel 2)**
  - § 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
  - § 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen
  - § 32 Meldepflichten
  - § 33 Registrierungspflicht
  - § 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten
  - § 35 Unterrichtungspflichten
  - § 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen
  - § 37 Ausnahmebescheid
  - § 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitun-gen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
    (*Entwurf vom 07.05.2024: „Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen*)
  - § 39 Nachweispflichten für Betreiber kritischer Anlagen
  - § 40 Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen
  - § 41 Untersagung des Einsatzes kritischer Komponenten
  - § 42 Auskunftsverlangen
  - **ACHTUNG: Normspezifische Prüfung des Regelungsadressaten!**

12

NIS-2-Umsetzung: Pflichten für § 28-Unternehmen

- **§ 30 BSIG-RegE: Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen**
- *„(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet,* ***geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die durch Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit*** *der informationstechnischen Systeme, Komponenten und Prozesse,* ***die sie für die Erbringung ihrer Dienste nutzen****, zu* ***vermeiden*** *und* ***Auswirkungen von Sicherheitsvorfällen möglichst gering*** *zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.* ***Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren****.*

  (2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen: [… ***10 Vorgaben des Abs. 2 …****]“*

  ➔ ***Vermeidung + „gering halten“ von Auswirkungen: Pflicht zum Risikomanagement***

  ➔ ***Pflicht zur Dokumentation***

  ➔ ***Explizite Einbeziehung der Lieferkette durch § 30 Abs. 2 Nr. 2 BSIG-RegE***

  ➔***Aber: keine generelle Pflicht zum proaktiven Nachweis gegenüber BSI***

  ➔***Als Einstieg??: CyberRisikoCheck nach DIN SPEC 27076 (siehe Website des BSI)***
- **§ 39 BSIG-RegE: Nachweispflichten (nur) für Betreiber kritischer Anlagen**

13

NIS-2-Umsetzung: Pflichten für § 28-Unternehmen

- **§ 38 BSIG-RegE: Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen**
  - **Umsetzung und Überwachung der Umsetzung von Maßnahmen nach § 30 BSIG-RegE durch Geschäftsleitung (Abs. 1)**

    „Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen ~~im Bereich der Cybersicherheit zu billigen~~ umzusetzen und ihre Um-setzung zu überwachen.“ (Vgl. zu RefE vom 07.05.2024)
  - **Ausschluss der Enthaftung der Geschäftsleitung (Abs. 2)**

    „Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Ein-richtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.
    *(**ReFE vom 07.05.2024:** „Ein Verzicht der Einrichtung auf Ersatzansprüche […] ist unwirksam. […]“)*
  - **Pflicht zur Teilnahme der Geschäftsleitung an Schulungen (Abs. 3)**

    „Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben.“

14

NIS-2-Umsetzung: Pflichten für § 28-Unternehmen
- EXKURS -

- **§ 32 BSIG-RegE: Meldepflichten**
  - **zeitlich dreifach gestufte Meldepflicht an gemeinsame Meldestelle des BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Abs. 1)**
  - **1. Stufe:** *„1. **unverzüglich, spätestens jedoch innerhalb von 24 Stunden** nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, […]“*
  - **2. Stufe:** *„2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen Sicherheitsvorfall, in der […] “*
  - **Zwischenmeldung auf Anforderung des BSI (Abs. 1 Nr. 3)**
  - **3. Stufe:** *„4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält: […]“*

    „Dauert der Sicherheitsvorfall zum im Absatz 1 Nummer 4 genannten Zeitpunkt noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung vor. Die Abschlussmeldung ist dann innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls vorzulegen.“
  - **Festlegung der Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte durch BSI (Abs. 4)**
- **§ 35 BSIG-RegE: Unterrichtungspflichten:** Anordnung der Unterrichtung der Betroffenen
- **§ 36 BSIG-RegE: Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen:** Unterrichtung der Öffentlichkeit (Abs. 2)
- **Achtung:** Keine Ersetzung der Pflichten der Artt. 33, 34 DS-GVO

15

NIS-2-Umsetzung: Pflichten für § 28-Unternehmen
- EXKURS zum Nachlesen -

- **§ 33 BSIG-RegE: Registrierungspflicht**
  - **Registrierungspflicht nach Abs. 1**

    *„Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, **spätestens drei Monate, nachdem** sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit folgenden Angaben zu übermitteln: […] “*
  - **Weitere Informationen durch Betreiber kritischer Anlagen (Abs. 2)**
  - **Registrierung des Betroffenen durch BSI bei Nicht-Registrierung (Abs. 3)**
  - **Pflicht zur Vorlage von Dokumenten (Abs. 4)**

    „Rechtfertigen Tatsachen die Annahme, dass eine Einrichtung ihre Pflicht zur Registrierung nach Absatz 1 oder 2 nicht erfüllt, so hat diese dem Bundesamt auf Verlangen die aus Sicht des Bundesamtes für die Bewertung erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.“
  - **Aktualisierungspflicht (Abs. 5)**

    „Bei Änderungen der nach Absatz 1 oder 2 zu übermittelnden Angaben sind dem Bundesamt geänderte Versorgungskennzahlen einmal jährlich zu übermitteln und alle an-deren Angaben unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von der Änderung erhalten hat, zu übermitteln.“
  - **Festlegung der Einzelheiten zur Ausgestaltung durch BSI (Abs. 6)**

16

Agenda

- Von der Richtlinie zur Umsetzung
- Wer ist betroffen?
- Pflichten für § 28-Unternehmen
- **Exkurs: Verhältnis zur DS-GVO**
- Fragen und Diskussion

17

NIS-2-Umsetzung: Verhältnis zur DS-GVO

- **Anwendungsbereich: (automatisierte) Verarbeitung von personenbezogenen Daten**
  - **Personenbezug: sog. relativer Ansatz** (EuG, Urt. v. 26.4.2023, Rs. T-557/20)
- **Artt. 6, 5 Abs. 1 lit. a, Abs.2 DS-GVO – m.a.W.: Keine Verarbeitung personenbezogener Daten ohne dokumentierte Rechtsgrundlage**
  - **Auslegungshilfe?: ErwGr. 121 NIS-2 Richtlinie** mit Bezug auf Art. 6 Abs. 1 UAbs. 1 lit. c, Abs. 3 und Abs. 1 UAbs. 1 lit. f DS-GVO
  - **Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO (Erfüllung einer gesetzlichen Pflicht)**
    - Risiko: Zirkelschluss mit „Zweck heiligt die Mittel“
    - Anforderungen von Art. 6 Abs. 2, 3 DS-GVO
    - **Problem??: Erfüllung einer noch nicht geltenden gesetzlichen Pflicht??**
  - **Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO (Interessenabwägung)**
    - sachgerecht und dynamisch - aber: keine Rechtsgrundlage für Behörden
  - **Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, § 26 Abs. 1 S. 1 BDSG (Vertragserfüllung)**
  - **Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO, § 26 Abs. 2 BDSG (Einwilligung)**
  - **Art. 6 Abs. 4 i. V. m. Abs. 1 DS-GVO (vgl. ErwGr. 50 DS-GVO)**
    - Relevanz der Datenschutzhinweise?!
- **Proaktive Transparenzpflicht nach Artt. 13, 14 DS-GVO**
- **Auskunftsanspruch nach Art. 15 DS-GVO**

18

Agenda

- Von der Richtlinie zur Umsetzung
- Wer ist betroffen?
- Pflichten für § 28-Unternehmen
- Exkurs: Verhältnis zur DS-GVO
- **Fragen und Diskussion**

19

Fragen und Diskussion!

Rechtsanwalt Dr. Jens Eckhardt
Fachanwalt für IT-Recht
Datenschutz-Auditor (TÜV)
IT-Compliance Manager (TÜV)

Erkrather Straße 162
40233 Düsseldorf
Tel.: +49 211 – 30 14 66 90
eckhardt@pitc-legal.de
www.pitc-legal.de

[pitc] legal Eckhardt Rechtsanwälte Partnerschaft mbB
privacy - information technology - compliance

20

Rechtsanwalt Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht

Datenschutz-Auditor (TÜV) und IT-Compliance Manager (TÜV)

Eckhardt Rechtsanwälte Partnerschaft mbB – www.pitc-legal.de

Seit 2001 berät er bundesweit nationale und internationale Unternehmen zu den Themen Datenschutz, Informationstechnologie, Telekommunikation und Marketing. Die Beratung umfasst die gerichtliche Vertretung, Vertretung gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, die strategische Beratung bei der Einführung neuer Systeme, die Bewertung von bestehenden Systemen, das Outsourcing sowie die Vertragsgestaltung.

Funktionen als:

- Datenschutztag (Computas GmbH), Moderation und Mit-Gestaltung der Tageskonferenz seit 2010
- Dozent zum Datenschutzrecht der udis Ulmer Akademie für Datenschutz und IT-Sicherheit – gemeinnützige Gesellschaft mbH
- Mitglied im Vorstand des Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (Ressort Recht)
- Mitglied im Vorstand von EuroCloud Deutschland_eco e.V. (Ressort Recht)
- Lehrbeauftragter der SRH Fernhochschule Riedlingen zum Internet- und Medienrecht und Datenschutz sowie Lehrbeauftragter zum Datenschutzrecht
- Mitglied im Wissenschaftsberat der Zeitschrift „Recht der Datenverarbeitung", Datakontext Verlag
- Mitglied im Wissenschaftsberat der Zeitschrift ZD, Verlag C.H. Beck
- Anhörung durch die Datenschutzaufsichtsbehörden als Fachexperte für Werbung und Adresshandel
- DeutscherDialogmarketingVerband. Leitung des Arbeitskreises Datenschutz
- Moderator und Referent verschiedener Datenschutzveranstaltungen und Autor von Fachbeiträgen zum Datenschutz-, IT-, Zivil- und Wettbewerbsrecht und zur Datenschutz-Grundverordnung, - auch zusammen mit Vertreter/innen deutscher Datenschutzaufsichtsbehörden

Podcast von Dr. Jens Eckhardt:

Otto Schmidt live, Podcast „Datenschutzrecht", Verlag Dr. Otto Schmidt Köln

[pitc legal] Eckhardt Rechtsanwälte Partnerschaft mbB

Auswahl der Veröffentlichungen:

- **AI Act und EU-Datenstrategie , Verlag Datev eG, Nürnberg, in Erstellung**
- **EU-Datenrecht, AI Act und Cyber Security Regulation, PrivacyXperts Verlag, in Erstellung**
- Datenverarbeitung in Drittstaaten, Eckhardt/Fuhlert, 2024, PrivacyXperts Verlag
- Buch „Websites, Cookies & Co., TTDSG", 2023, Verlag Datev eG, Nürnberg
- „Datenschutz und Personalisierung – (k)ein Widerspruch" in den Buch „Leitfaden Personalisierung – Mehr Umsatz mit Marketing Automation", Verlag Marketing Börse GmbH
- Schwartmann/Jaspers/Eckhardt, Kommentar zum TTDSG, 2022, C.F. Müller Verlag
- TTDSG leicht erklärt, 2021, PrivacyXperts Verlag
- GDPR Playbook, 2020, eco - Verband der Internetwirtschaft e.V., Autor der Kapitel Cloud Computing und E-Mail-Marketing
- Datenschutz&Marketing – Praxisleitfaden, PrivacyXperts Verlag, 2019, ISBN 978-3-8125-2792-7
- Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, C.H. Beck München, 2025
- Leitfaden – Datenschutz und Cloud Computing, Mitautor und Leiter der Taskforce „Datenschutz" der AG „Rechtsrahmen im Cloud Computing", Trusted Cloud-Initiative des BMWi
- Bergmann/Möhrle/Herb, BDSG/DS-GVO , Mit-Autor, Boorberg Verlag
- Recht der elektronischen Medien, Kommentar, Mitautor, C. H. Beck München
- Handbuch IT- und Datenschutzrecht, Mitautor, Verlag C. H. Beck München, u.a. NIS-Richtlinien und Umsetzung im BSI-Gesetz, Cyber Resilience Act
- Beck'scher OK, Wolff/Brink, BDSG/DS-GVO , Mit-Autor, C.H. Beck München
- Beck'scher TKG Kommentar, Mitautor, C. H. Beck München, u.a. Öffentliche Sicherheit und Sicherheit
- Digitalisierung und Transformation im Unternehmen, Mitautor, KS-Energy
- Leitfaden zu Durchsuchung und Beschlagnahme, Herausgeber und Mit-Autor, EuroCloud Deutschland_eco e.V.

21