DuD 2025

NIS-2 – Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht

Potsdam, 02.6.2025

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

1

Agenda

- Umsetzung der NIS-2-Richtlinie
- Anforderungen der DS-GVO: Eckpunkte
- NIS-2-Richtlinie vs. Datenschutzrecht
- Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht
- Fragen und Diskussion

2

Umsetzung der NIS-2-Richtlinie

- **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: 26.11.2024))
  - **EU-Richtline: Umsetzungsbedarf durch nationales Recht**
  - **Inkrafttreten:** 16. Januar 2023 – **Umsetzungsfrist bis:** 17. Oktober 2024
- Umsetzung durch: **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz**
  - **Regierungsentwurf: BT-Drs. 20/13184 vom 02.10.2024:** https://dserver.bundestag.de/btd/20/131/2013184.pdf (Stand des Links: 28.02.2025)
  - **sog. Artikel-Gesetz**
  - **Inkrafttreten: Tag nach der Verkündung (Art. 33) = KEINE Umsetzungsfrist**
    - Registrierungspflicht (§ 33 BSIG-RegE): binnen 3 Monaten ≠ Übergangsregelung
  - **BSIG-Regierungsentwurf - 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)

3

Umsetzung der NIS-2-Richtlinie

- **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: 26.11.2024))
  - **EU-Richtline: Umsetzungsbedarf durch nationales Recht**
  - **Inkrafttreten:** 16. Januar 2023 – **Umsetzungsfrist bis:** 17. Oktober 2024
- Umsetzung durch: **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz**
  - **Regierungsentwurf: BT-Drs. 20/13184 vom 02.10.2024:** https://dserver.bundestag.de/btd/20/131/2013184.pdf (Stand des Links: 28.02.2025)
  - **sog. Artikel-Gesetz**
  - **Inkrafttreten: Tag nach der Verkündung (Art. 33) = KEINE Umsetzungsfrist**
    - Registrierungspflicht (§ 33 BSIG-RegE): binnen 3 Monaten ≠ Übergangsregelung
  - **BSIG-Regierungsentwurf - 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)

4

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

- **Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen –** § 30 BSIG-RegE zur **Umsetzung des Art. 21 NIS-2-Richtlinie**

  „(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 durch technische und organisatorische Maßnahmen***
  - ➔ ***Pflicht zur Dokumentation***
  - ➔ ***aber: keine generelle Pflicht zum proaktiven Nachweis gegenüber BSI***
  - ➔ ***Parallelen zu Art. 32 DS-GVO, aber keine Gleichheit***
  - ○ *Exkurs:* § 39 BSIG-RegE: Nachweispflichten für Betreiber kritischer Anlagen

5

Agenda

- Umsetzung der NIS-2-Richtlinie
- **Anforderungen der DS-GVO: Eckpunkte**
- NIS-2-Richtlinie vs. Datenschutzrecht
- Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht
- Fragen und Diskussion

6

Anforderungen der DS-GVO: Eckpunkte

- **Anwendungsbereich: (automatisierte) Verarbeitung von personenbezogenen Daten**
  - **Personenbezug: sog. relativer Ansatz** (vgl. EuG, Urt. v. 26.4.2023, Rs. T-557/20)
- **Artt. 6, 5 Abs. 1 lit. a, Abs. 2 DS-GVO – m.a.W.: Erfordernis einer Rechtsgrundlage**
  - Numerus Clausus der Rechtsgrundlagen in Art. 6 DS-GVO: **BSIG-neu ≠ Rechtsgrundlage**
  - **Die Qual der Wahl – oder: Ausnahmecharakter neben Einwilligung gemäß EuGH**
  - Art. 6 Abs. 1 UAbs. 1 lit. b bis f DS-GVO: **Erforderlichkeit im Sinne von EuGH, Urt. v. 09.01.2025, Rs. C-394/23 – SNCF** (dort Rn. 28)
  - **Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO (Erfüllung einer gesetzlichen Pflicht):** Zirkelschluss?
    - Anforderungen von Art. 6 Abs. 2, 3 DS-GVO
  - **Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO (Interessenabwägung)** (nicht für Behörden)
    - sachgerecht und dynamisch, aber nicht statisch
  - **Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, § 26 Abs. 1 S. 1 BDSG (Vertragserfüllung)**
    - Schutz als Vertragsgenstand gegenüber betr. Person, aber jedenfalls Nebenpflicht
    - aber: keine Berechtigung aus Drittvertragsverhältnissen („NIS-Sicherheitsvertrag“)
  - **Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO, § 26 Abs. 2 BDSG (Einwilligung)**
    - Transparenz im Sinne von Art. 4 Nr. 11 DS-GVO – statische Einwilligung?
    - Freie Widerrufbarkeit (Art. 7 Abs. 3 DS-GVO)
  - **Art. 6 Abs. 4 i. V. m. Abs. 1 DS-GVO (vgl. ErwGr. 50 DS-GVO)**

7

Anforderungen der DS-GVO: Eckpunkte

- **Proaktive Transparenzpflicht nach Artt. 13, 14 DS-GVO - insbesondere**
  - *„die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung“ (Art. 13 Abs. 1 lit. c)*
  - ***„wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht**, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden“ (Art. 13 Abs. 1 lit. d)*

  ➔ ***Herausforderung in der Praxis?!: Zusammenfassung bezüglich BSIG, DORA, CSA, CRA & Co.***

- **Auskunftsanspruch nach Art. 15 DS-GVO**
  - personenbezogene Daten, Zwecke, Empfänger, Dauer (Art. 15 Abs. 1)
  - Kopie der personenbezogenen Daten (Art. 15 Abs. 3 DS-GVO)
  - Rechtsprechung (BGH, Urt. v. 15.06.2021, VI ZR 576/19 (Umfassende Reichweite); EuGH, Urt. v. 12.01.2023, Rs. C-154/21 (Empfänger); EuGH, Urt. v. 04.05.2023, Rs. C-487/21 (Kopie))

8

Agenda

- Umsetzung der NIS-2-Richtlinie
- Anforderungen der DS-GVO: Eckpunkte
- **NIS-2-Richtlinie vs. Datenschutzrecht**
- Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht
- Fragen und Diskussion

9

NIS-2-Richtlinie vs. Datenschutzrecht

- **Verhältnis zur DS-GVO**
  - **BSIG-RegE**
    - Keine explizite Aussage zum Rangverhältnis
    - **Vorrang der DS-GVO als EU-Verordnung**
    - DS-GVO: keine Öffnungsklausel → BSIG-neu ≠ Rechtsgrundlage i.S.d. DS-GVO
  - **Auslegung im Lichte der NIS-2 Richtlinie**
    - **ErwGr. 14: *„… lässt … unberührt*“ Datenschutzrecht**
    - **ErwGr. 43: *„im Einklang mit*“**
    - weitere Bezugnahmen auf die DS-GVO

- **Weiterführendes:**
  - *Eckhardt, „NIS: Was gilt wann?“, Datenschutz-PRAXIS, 09/2024, S. 5 ff.*
  - *Eckhardt, „Rechtsgrundlagen zur Umsetzung der NIS-2-Richtlinie“, Datenschutz-PRAXIS, 03/2025, S. 1 ff.*
  - *Eckhardt, „NIS-2-Pflichten und DSGVO: Parallelitäten und Unterschiede“, Datenschutz-PRAXIS, demnächst*

10

NIS-2-Richtlinie vs. Datenschutzrecht

- **Rechtsgrundlage: Erwägungsgrund 121 NIS-2-Richtlinie**

  *„Die Verarbeitung personenbezogener Daten […] in dem **zur Gewährleistung der Sicherheit von Netz- und Informationssystemen** erforderlichen und verhältnismäßigen Umfang könnte auf der Grundlage als rechtmäßig angesehen werden, dass diese Verarbeitung einer rechtlichen Verpflichtung entspricht, der der Verantwortliche **gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679** unterliegt. Die Verarbeitung personenbezogener Daten könnte **auch für berechtigte Interessen** erforderlich sein, die […] **gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679** wahrgenommen werden, auch wenn eine solche Verarbeitung für Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder die freiwillige Mitteilung relevanter Informationen gemäß dieser Richtlinie erforderlich ist. […] […] gemäß Artikel 6 Absatz 1 Buchstabe c oder e und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 übertragen wurde, oder zur Verfolgung eines berechtigten Interesses der wesentlichen und wichtigen Einrichtungen gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung. […] .“*

  - Bindungswirkung der NIS-2-Richtlinie zur Anwendung der DS-GVO?
  - **Erfüllung der konkreten NIS-2-RiLi-Pflichten: Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO**
  - **im Übrigen: Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO**

11

Agenda

- Umsetzung der NIS-2-Richtlinie
- Anforderungen der DS-GVO: Eckpunkte
- NIS-2-Richtlinie vs. Datenschutzrecht
- **Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht**
- Fragen und Diskussion

12

Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht

- **Herausforderung in der Praxis**
  - **Keine Umsetzungsfrist nach Inkrafttreten des BSIG-neu**
  - **ABER:** Umsetzung der technischen und organisatorischen Maßnahmen (einschließlich Verarbeitung personenbezogener Daten hierfür) **vor Geltungsbeginn** der Rechtspflicht

  ➔ **Umsetzung einer Rechtspflicht ohne Rechtspflicht**

- **Relevanz:** Art. 82 DS-GVO?, Art. 83 DS-GVO? und Maßnahmen der Artt. 57, 58 DS-GVO?

- **Rechtsgrundlage der DS-GVO**
  - ab Geltungsbeginn: Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO
  - Zeitraum zwischen Umsetzungsbeginn und Geltung der Pflicht?
    - Art. 6 Abs. 1 UAbs. 1 **lit. c** DS-GVO **oder**
    - Art. 6 Abs. 1 UAbs. 1 **lit. f** DS-GVO
    - Herausforderung insbesondere: Transparenzpflicht nach Artt. 13, 14 DS-GVO

  ➔**Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO auch vor Geltungsbeginn, sofern hinreichend konkrete Pflicht (siehe Art. 6 Abs. 2 und Abs. 3 DS-GVO)**

Agenda

- Umsetzung der NIS-2-Richtlinie
- Anforderungen der DS-GVO: Eckpunkte
- NIS-2-Richtlinie vs. Datenschutzrecht
- Rechtsgrundlage zur Umsetzung einer Rechtspflicht ohne Rechtspflicht
- **Fragen und Diskussion**

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

15

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.

16