BvD e.V.

Blitzlicht EU-ACTionism – Behalten Sie den Überblick (AI Act, DA, DSA, DMA, DGA, NIS &Co.)

online, 01.02.2024

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

1

Agenda

- Überblick
- Digital Services Act (DSA)
- Data Act (DA), Digital Governance Act (DGA)
- Digital Market Act (DMA)
- Artificial Intelligence Act & AI Liability Directive
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- Rolle des Datenschutzbeauftragten?

2

Überblick

Datenschutz (Privacy)	DS-GVO (plus BDSG) ePrivacy-RiLi (zukünftig?: ePrivacy-VO)	zukünftig?!: Beschäftigtendatenschutz-gesetz
Daten		Data Act Data Governance Act (DGA)
Digitale Dienste	Digital Services Act (DSA) Digital Market Act (DMA)	Health Data Spaces Regulation
Cyber Security	Cybersecurity Act (CSA) NIS 2 Directive Resilience of Critical Entities (CER)	Cyber Resilience Act (CRA) Digital Operational Resilience Act (DORA) Cyber Solidarity Act
Artificial Intelligence	AI Act	AI Liability Directive

3

Überblick

Datenschutz (Privacy)	DS-GVO (plus BDSG) ePrivacy-RiLi (zukünftig?: ePrivacy-VO)	zukünftig?!: Beschäftigtendatenschutz-gesetz
Daten		Data Act Data Governance Act (DGA)
Digitale Dienste	Digital Services Act (DSA) Digital Market Act (DMA)	Health Data Spaces Regulation
Cyber Security	Cybersecurity Act (CSA) NIS 2 Directive Resilience of Critical Entities (CER)	Cyber Resilience Act (CRA) Digital Operational Resilience Act (DORA) Cyber Solidarity Act
Artificial Intelligence	AI Act	AI Liability Directive

Ist das alles...?

4

Agenda

- Überblick
- **Digital Services Act (DSA)**
- Data Act (DA), Digital Governance Act (DGA)
- Digital Market Act (DMA)
- Artificial Intelligence Act & AI Liability Directive
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- Rolle des Datenschutzbeauftragten?

Digital Services Act (DSA)

- **Digital Services Act (DSA)**
  - **Gesetz über digitale Dienste (Verordnung (EU) 2022/2065 vom 19.10.2022)**
  - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065 (Stand: 31.01.2024)
  - **national ergänzend:** Digitale-Dienste-Gesetz (DDG)-Entwurf (= Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 …. und … Verordnung (EU) 2019/1150 ….) (https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/gesetz-durchfuehrung-verordnung-binnenmarkt-digitale-dienste.pdf?__blob=publicationFile (Stand: 31.01.2024))
  - **Inkrafttreten:** November 2022 – **Umsetzungsfrist bis:** 17.02.2024
- **Ziel:** Verschärfung von Sanktionen bei Verbreitung illegaler Inhalte
- **Verpflichtete: Anbieter von Vermittlungsdiensten (Intermediäre), insbes:** Hosting-, Caching- und Access-Provider, sehr große Online Plattformen (VLOP), sehr große Online Suchmaschinen (VLOSE)
- **Inhalt**
  - Schutz vor missbräuchlicher Verwendung der Plattform, Transparenzenpflichten bei Empfehlungssysteme, Pflicht zur Löschung illegaler Inhalte „im Internet“, Anzeigepflicht bei schweren Straftaten, Schadensersatz bei DSA-Verstößen, **Transparenz in Bezug auf Monetarisierung von Daten**, **Verbot von personalisierter Werbung mit Daten von Minderjährigen** sowie **Profiling von Minderjährigen**, **Verboten von personalisierter Werbung mittels besonderer Kategorien personenbezogener Daten**
  - **ErwGr. 10: Datenschutzrecht *„unberührt lassen“***

Agenda

- Überblick
- Digital Services Act (DSA)
- **Data Act (DA), Digital Governance Act (DGA)**
- Digital Market Act (DMA)
- Artificial Intelligence Act & AI Liability Directive
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- Rolle des Datenschutzbeauftragten?

Data Act (DA)

- **Data Act (DA)**
  - **Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datenverordnung)** vom 13.12.2023
  - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202302854 (Stand: 31.01.2024)
  - **Inkrafttreten:** Januar 2024 – **Geltung ab:** 12.09.2025 plus weitere Abstufungen in Art. 50 DA
- **Ziel:** Fairness in Bezug auf Daten im Sinne von Zugang und Nutzung von (auch fremden) Daten
- **Verpflichtete:** Hersteller, Eigentümer, Besitzer und Verwender von IoT-Geräten sowie Dritt-Nutzer der Daten aus IoT-Geräten (Marktortprinzip) (Internet der Dinge (IoT), Smart Devices sowie Waren mit digitalen Elementen (bspw. Kühlschränke mit Internetzugang, Autos)
- **Inhalt:**
  - **Zugang zu den Daten sowie Auswertung und Weitergabe an Dritte**
  - **ErwGr. 7:** *„[…] Die vorliegende Verordnung ergänzt das Unionsrecht zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre, insbesondere die Verordnungen (EU) 2016/679 und (EU) 2018/1725 und die Richtlinie 2002/58/EG, und **lässt es unberührt**. Keine Bestimmung dieser Verordnung **sollte dahingehend angewandt oder ausgelegt werden, dass** das Recht auf den Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation **abgeschwächt oder eingeschränkt wird**. …, einschließlich dem Erfordernis einer gültigen Rechtsgrundlage … . **Die vorliegende Verordnung stellt keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber dar.** Die **vorliegende Verordnung verpflichtet die Dateninhaber, Nutzern Dritten seiner Wahl oder auf Anfrage eines Nutzers personenbezogene Daten bereitzustellen**. […] "*

Digital Governance Act (DGA)

- **Digital Governance Act (DGA)**
  - **Daten- Governance-Rechtsakt** (Verordnung (EU) 2022/868 vom 30.05.2022)
  - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0868 (Stand: 31.01.2024)
  - **Inkrafttreten:** 23.06.2022 – **Umsetzungsfrist bis:** September 2023
- **Ziel: Stärkung des** Vertrauens in den Datenaustausch, Stärkung der Mechanismen zur Erhöhung der Datenverfügbarkeit, Überwinden von technischen Hindernissen für die Weiterverwendung von Daten
- **Verpflichtete:** Öffentliche Stelle („Öffentliche Hand"), Datenintermediäre, Datenaltruistischen Unternehmen
- **Inhalt**
  - Weiterverwendung von (geschützten) Daten im „Besitz" öffentlicher Stellen
  - **ErwGr. 4: Datenschutzrecht *„unberührt lassen"***

Agenda

- Überblick
- Digital Services Act (DSA)
- Data Act (DA), Digital Governance Act (DGA)
- **Digital Market Act (DMA)**
- Artificial Intelligence Act & AI Liability Directive
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- Rolle des Datenschutzbeauftragten?

Digital Market Act (DMA)

- **Digital Market Act (DMA)**
  - **Gesetz über digitale Märkte** (Verordnung (EU) 2022/1925 vom 14.09.2022)
  - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925 (Stand: 31.01.2024)
  - **Geltung seit:** 02.05.2023
- **Ziel:** Schutz vor Missbrauch der Machtposition durch große Online-Plattformen
  - „Kartellrechtlicher" Ansatz neben GWB
- **Verpflichtete: sog. Gatekeeper**
  - **EU-Kommission:** Benennung dieser Gatekeeper (https://digital-markets-act-cases.ec.europa.eu/gatekeepers (Stand: 31.01.2024)) (bspw. Alphabet Inc.)
- **Inhalt**
  - Verbot von Meistbegünstigungsklauseln, Verbot bestimmter Bindungen und Kopplungen, Auskunftsrecht für Werbetreibende und Verlage, **Verbot der Zusammenführung von Nutzerdaten über verschiedene Plattformen des Gatekeepers**, Transparenz in Bezug auf Preiszusammenstellungen, **Transparenz in Bezug auf Algorithmen der Werbedienste der Gatekeeper**
  - **ErwGr. 12: *„Zudem sollte diese Verordnung unbeschadet der Vorschriften gelten, die sich aus anderen Rechtsakten …* " VO 2016/679 und RiLi 2002/58/EG**

Agenda

- Überblick
- Digital Services Act (DSA)
- Data Act (DA), Digital Governance Act (DGA)
- Digital Market Act (DMA)
- **Artificial Intelligence Act & AI Liability Directive**
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- Rolle des Datenschutzbeauftragten?

Artificial Intelligence Act & AI Liability Directive

- **Artificial Intelligence Act (AI Act)**
  - **Gesetz über Künstliche Intelligenz**
  - Vorschlag vom 21.04.2021: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF (Stand: 31.01.2024)
  - **Status:** unklar, Einigung der Unterhändler des Europaparlaments und der EU-Staaten am 08.12.2023, aber nicht kein finaler Beschluss
  - **ergänzend:** Entwurf einer **Artificial Intelligence Liability Directive** (https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf (Stand: 31.01.2024))
- **Ziel:** Schaffung von Rahmenbedingungen für sichere Entwicklung, Vertrieb und Verwendung von „KI-Systemen“
- **Verpflichtete:** (vereinfacht) Anbieter und Nutzer der erfassten AI
- **Inhalt**
  - Regulierung durch Verbot von KI-Systemen mit besonders hohem Risikopotential, Regulierung von Systemen mit hohem Risiko, Transparenzverpflichtungen für Systeme mit geringen Risiken
  - **Entwurfsbegründung: Datenschutzrecht „bleiben unberührt“**
  - **ErwGr. 24, 72: „*im Einklang mit*“ (bestimmten Regelungen des) Datenschutzrecht**

Agenda

- Überblick
- Digital Services Act (DSA)
- Data Act (DA), Digital Governance Act (DGA)
- Digital Market Act (DMA)
- Artificial Intelligence Act & AI Liability Directive
- **NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)**
- Rolle des Datenschutzbeauftragten?

NIS-2-Richtlinie

- **NIS 2 Directive**
  - **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: 31.01.2024)
  - **Inkrafttreten:** 16. Januar 2023 – **Umsetzungsfrist bis:** 18. Oktober 2024
- **Ziel:** Stärkung des Schutzes bestimmter Einrichtungen und Diensten vor Cybergefahren entsprechend der aktuellen Cyberbedrohungslage
- **Verpflichtete:** Unternehmen ab der Größe eines mittleren Unternehmens in den gelisteten Wirtschaftssektoren (sog. size-cap-rule) (mittlere Unternehmen = mindestens 50 Beschäftigte oder mehr als 10 Mio. Jahresumsatz bzw. Jahresbilanzsumme)
  - Konkretisierung der Festlegung und des Ob durch Rechtsverordnung des BMI
- **Inhalt**
  - toM zum Schutz der IT-Systeme und -Prozesse, Meldung von Sicherheitsvorfällen an BSI (u.a. Erstmeldung innerhalb von 24 Stunden), Nachweisführung gegenüber dem BSI über die Erfüllung bestimmter Sicherheitsanforderungen
  - Aufhebung der NIS-Richtlinie (Richtlinie (EU) 2016/1148) und Änderung der eIDAS-VO sowie EECC-Richtlinie
  - **ErwGr. 14: *„… lässt … unberührt“* Datenschutzrecht; ErwGr. 43: *„im Einklang mit“* sowie mehrfache Bezugnahmen auf die DS-GVO**

Cyber Resilience ACT (CRA)

- **Cyber Resilience ACT (CRA)**
  - **Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung** (EU) 2019/1020
  - **Entwurf vom 15.09.2022:** https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0020.02/DOC_1&format=PDF[Link (Stand: 31.01.2024)]
  - **Status:** Gesetzgebungsverfahren
- **Ziel:** Verbesserung der Cybersicherheit von Produkten mit digitalen Elementen zum Schutz der Nutzer
- **Verpflichtete:** Hersteller, Händler und Importeure von Produkten mit digitalen Elementen
- **Inhalt**
  - Erfassung von Software und Hardware mit Möglichkeit zum Zugriff hierauf mittels eines Produkt oder Netzwerks - nicht: digitale Dienste (bspw. SaaS), nicht geschäfltcher OSS
  - Transparenz sowie Dokumentation und ständige Bewertung von Cybersicherheitsrisiken, Verbot des Inverkehrbringens von Produkten mit bekannten Schwachstellen, Sicherheit durch Standardkonfiguration (Security by Design), Schutz vor unbefugtem Zugriff, Minimierung der Angriffsflächen, Minimierung der Auswirkungen von Sicherheitszwischenfällen sowie Vertraulichkeit von Daten durch Verschlüsselung, Schutz der Datenintegrität und Datenminimierung
  - **Erleichterung der Einhaltung der DS-GVO, Geltung des CRA *„unbeschadet der Verordnung (EU) 2016/679“***

Digital Operational Resilience Act (DORA)

- **Digital Operational Resilience Act (DORA)**
  - **Verordnung über die digitale operationale Resilienz im Finanzsektor** (EU) 2022/2554 vom 14.12.2022
  - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (Stand: 31.01.2024)
  - **Inkrafttreten:** 17.01.2023 – **Umsetzungsfrist bis:** 17.01.2025
  - **ergänzend national:** Finanzmarktdigitalisierungsgesetz (FinmadiG)-Entwurf vom 22.12.2023
- **Ziel:** Verbesserung der digitalen operationalen Widerstandsfähigkeit von EU-Finanzunternehmen und deren IKT-Dienstleistern sowie Schaffung eines EU-weit einheitlichen Aufsichtsrahmens
- **Verpflichtete: Finanzunternehmen (einschließlich E-Geld und Versicherungen) und IKT-Dienstleister i.S.d. Art. 2 DORA**
- **Inhalt**
  - insbesondere Etablierung eines Überwachungs- und Risikomanagements von ITK-Dienstleistern, Gestaltung von Richtlinien zur Informationssicherheit, IKT-Geschäftsfortführungsleitlinie, Prozesses zur Identifizierung, Klassifizierung, Behandlung und Meldung von Cyberbedrohungen und -vorfällen sowie IKT-Störfällen, Durchführung von regelmäßigen Tests zur Überprüfung der digitalen operativen Resilienz
  - **Art. 56 Abs. 1 S. 2 DORA: *„im Einklang stehen“* mit Datenschutzrecht - Betonung von Art. 6 DS-GVO durch ErwGr. 34 DORA**

Agenda

- Überblick
- Digital Services Act (DSA)
- Data Act (DA), Digital Governance Act (DGA)
- Digital Market Act (DMA)
- Artificial Intelligence Act & AI Liability Directive
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- **Rolle des Datenschutzbeauftragten?**

Rolle des Datenschutzbeauftragten?

- **Festlegung der Aufgaben durch Artt. 37 bis 39 DS-GVO**
  - im Kern: Überwachung und Beratung bei Umsetzung und Einhaltung des Datenschutzrechts (Art. 39 Abs. 1 DS-GVO)
  - Art. 35 Abs. 2 DS-GVO: Rat des DSB bei DSFA
- **Rolle im Kontext der neuen Digitalgesetzgebung**
  - **Unterstützung:** im Rahmen der Artt. 37 ff. DS-GVO bei der Umsetzung der Anforderungen
  - **Perspektive:** Umsetzung der DS-GVO, aber nicht primär Umsetzung der Vorgaben der Digitalgesetze
    - Umsetzung der Pflichten **mittelbar durch Verarbeitung personenbezogener Daten** (v.a. Cyber Security, Sperrpflichten, usw.) (Achtung: „Zweck heiligt nicht die Mittel!“)
    - Umsetzung der Pflichten **gerade durch Verarbeitung der pers. bez. Daten** (v.a. Sharing)
  - **Schnittpunkt zu den Digitalgesetzen**
    - Datenschutzrecht „bleibt unberührt“, „im Einklang mit“, usw.
    - Was heißt das? Nicht abschließend im Detail klar, aber vereinfacht: Vorrang der DS-GVO
    - ➔ Umsetzung der Digitalgesetze im Rahmen und auf der Grundlage der DS-GVO
  - ➔ **Datenschutzbeauftragter: Kenntnis und Verständnis der Digitalgesetze als Voraussetzung zur Bewertung und Unterstützung bei der Umsetzung aus der Perspektive der DS-GVO**
  - ➔ **Unternehmen: Auslegung und Festlegung der Anforderungen aus den Digitalgesetzen**

Agenda

- Überblick
- Digital Services Act (DSA)
- Data Act (DA), Digital Governance Act (DGA)
- Digital Market Act (DMA)
- Artificial Intelligence Act & AI Liability Directive
- NIS-2-Richtlinie, Cyber Resilience ACT (CRA) und Digital Operational Resilience Act (DORA)
- Rolle des Datenschutzbeauftragten?

Fragen und Diskussion!

Rechtsanwalt Dr. Jens Eckhardt

Fachanwalt für IT-Recht
Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV) und
IT-Compliance Manager (TÜV)

Immermannstraße 15
40210 Düsseldorf
Tel.: +49 211 – 30 14 66 90
eckhardt@pitc-legal.de
www.pitc-legal.de

Eckhardt Rechtsanwälte
Partnerschaft mbB
privacy - information technology - compliance

21

Rechtsanwalt Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV), Compliance-Officer (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:

- 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)
- Dozent der DeutscheAnwaltAkademie Gesellschaft für Aus- und Fortbildung sowie Serviceleistungen mbH (Fortbildung im Bereich Fachanwalt IT-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
- 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

Eckhardt Rechtsanwälte
Partnerschaft mbB

Auswahl der Veröffentlichungen:

- 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
- Datenverarbeitung in Drittstaaten, Eckhardt/Fuhlert, 2020, 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
- Mit-Autor „Vernetzte und autonome Mobilität", eco Verband der deutschen Internetwirtschaft, 2019
- Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, C.H. Beck München, 2022
- „Wann ist ein Datum ein personenbezogenes Datum?", gemeinsam mit Dr. Brink, ZD Editorial 1/2015 und ZD 2015, 205 ff.
- 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
- Beck'scher OK, Wolff/Brink, BDSG/DS-GVO , Mit-Autor, C.H. Beck München
- Beck'scher TKG Kommentar, Mitautor, C. H. Beck München
- Digitalisierung und Transformation im Unternehmen, Mitautor, KS-Energy
- Leitfaden zu Durchsuchung und Beschlagnahme, Herausgeber und Mit-Autor, EuroCloud Deutschland_eco e.V.

22