Das Zusammenspiel zwischen Data Act und DS-GVO

Datenschutz am Mittag

am 04.09.2025

Orchester der Digitalstrategie

Was will der DataAct?

Ziel:

Datenaustausch und Datennutzung fördern

- Datenzugangsrechte
- Erhöhung der Datenverfügbarkeit
- Freier und sicherer Datenverkehr im Einklang mit dem Schutz des Gemeinwohls
- Daten sollen auffindbar, zugänglich, interoperabel und weiterverwendbar sein

Was will die Datenschutzgrundverordnung?

Art. 1
Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Grundsatz der Datenminimierung

Datenminimierung heißt nicht Datenvermeidung um jeden Preis

Auf das für die Zwecke notwendige Maß beschränkt

So wenig wie möglich, so viel wie nötig erlaubt

Auseinandersetzung mit Verarbeitungsprozessen

Datenzugang und Datenbereitstellung

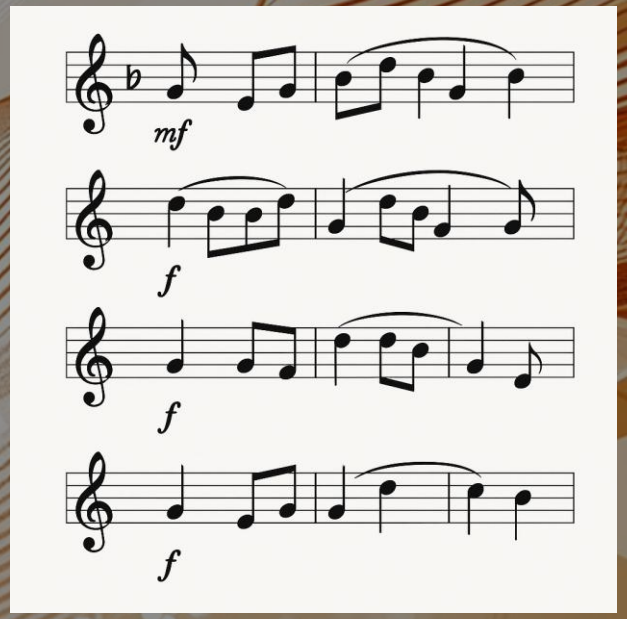
Akteure:

- Entwickler / Hersteller
- Dateninhaber
- Vertragspartner
- Nutzer – **zentrale Rolle**
- Dritten / Datenempfänger

Datenzugang und Datenbereitstellung

<u>Aufbau Kapitel II:</u>

- Faktischer Zugangsanspruch nach Art. 3 Abs. 1 DA
  - „Access by Design“
- Bereitstellungspflicht nach Art. 4 / 5 DA
  - „aktive“ Pflicht des Dateninhabers auf Verlangen
- Recht der Nutzer auf Weitergabe der Daten an Dritte



Datenzugang und Datenbereitstellung

Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen:

- Zugang und aktive Bereitstellung von Sensor- und Maschinendaten, die bei der Nutzung generiert werden, sowie den dazugehörigen Metadaten – „IoT- Daten“
- **Art. 4 Abs. 1 DA:**

*„Soweit der Nutzer **nicht direkt** vom vernetzten Produkt oder verbundenen Dienst aus auf die Daten zugreifen kann, **stellen die Dateninhaber** dem Nutzer **ohne Weiteres verfügbare Daten** einschließlich der zur Auslegung und Nutzung der Daten erforderlichen **Metadaten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format** und – falls relevant und technisch durchführbar – in der **gleichen Qualität** wie für den Dateninhaber **kontinuierlich und in Echtzeit bereit**. Dies geschieht auf einfaches Verlangen auf elektronischem Wege, soweit dies technisch durchführbar ist.“*

- **Art. 5 Abs. 1 DA:** „Auf Verlangen eines Nutzers oder einer im Namen eines Nutzers handelnden Partei stellt der Dateninhaber **einem Dritten** ohne Weiteres….“

- **Anwendungsbereich DS-GVO eröffnet?**

Personenbezogene Daten?

Smart- Home- Geräte:

Produkte:

Smarte Thermostate, Sprachassistenten, Türklingeln, Waschmaschinen, Kühlschränke,

PbD:

Sprachaufzeichnungen, Bewegungsprofile, Nutzungsgewohnheiten, Gerätestandort, Video- od. Audioaufnahmen von Personen

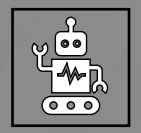
Vernetzte Fahrzeuge

Produkte:

Connected Cars, Flottenmanagement-Systeme, Fahrzeugdiagnose mit Remote Access

PbD:

Fahrverhalten, GPS-Daten/ Standortverlauf, Nutzerprofile, Diagnosedaten die auf individuelle Nutzung zurückzuführen sind



Industrieprodukte mit Nutzerbezug

Produkte:

IoT- Maschinen mit Bedienerlogins, Gebäudeautomatisierung (zB. Zugangssysteme, Zeiterfassung)

PbD: Logindaten, Benutzerkennungen, Standort des Einsatzes, Zeiterfassungsdaten (wann hat wer was bedient)

Mobilitätsdienste & Sharing-Produkte

Produkte:

E-Scooter/ E- Bike/ Car- Sharing, smarte Ladesäulen

PbD:

Bewegungsdaten, Abrechnungsdaten, Nutzerverhalten, Geräte- Id‘s in Verbindung mit Nutzerkonten

Energieprodukte

Produkte:

Intelligente Stromzähler, Photovoltaik mit Fernüberwachung, Energieverbrauchsmanagement- Systeme

PbD:

Verbraucherprofile von Haushalten. Nutzungszeitpunkte, Verhaltensanalysen

Sonstige

Produkte:

Smarte Fernseher, Fitnesstracker, Wearables, Spielekonsolen

PbD:

Gesundheitsdaten, Nutzungsverlauf, Standortdaten, Nutzerverhalten

Personenbezogene Daten

- Datenschutzrechtliche Grundsatzfragen!
- Auf wessen Kenntnis des Personenbezugs ist abzustellen?
- EuGH C-413/23 P – Entscheidung erwartet am 04.09.2025

- Genaue Bestimmung überhaupt möglich?
- Wie geht man mit gemischten Datensätzen um?
- Nutzung durch Privatpersonen oder jur. Personen?

- Bisher: im Zweifel Personenbezug +
- Künftig: Differenzierung, sofern möglich?
    - Im Zweifel aber auch weiterhin Personenbezug annehmen?(EG 7)

Wie ist das Zusammenspiel geregelt?

- Keine Datennutzungsverträge sondern Geltung DSGVO
- DSGVO gilt **vorrangig** - Bereitstellungspflicht nur insoweit bei pbD (Art. 1 Abs. 5 S. 3 DA)
- Datenschutzrechtliche Erlaubnis **erforderlich** (ggfs. + Art. 9 DS-GVO)
- keine **Abschwächung/Einschränkung** (ErwG. 7 S. 5 DA)
- ErwG. 7 DA:

  *„(…)Die vorliegende Verordnung stellt **keine Rechtsgrundlage** für die **Erhebung oder Generierung** personenbezogener Daten durch den Dateninhaber dar. (…)“*

Wie ist das Zusammenspiel geregelt?

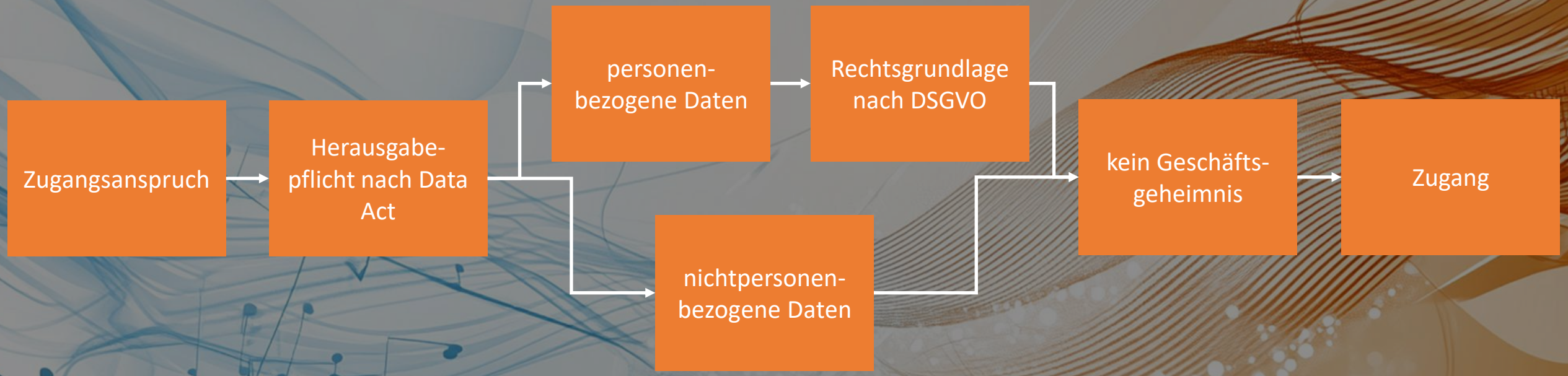
Art. 4 Abs. 12 DA:

*„Handelt es sich bei dem Nutzer **nicht** um die betroffene Person, deren personenbezogene Daten verlangt werden, so darf der Dateninhaber personenbezogene Daten, die bei der Nutzung eines vernetzten Produktes oder verbundenen Dienstes generiert werden, dem Nutzer **nur dann bereitstellen**, wenn es für die Verarbeitung eine **gültige Rechtsgrundlage gemäß Artikel 6 der Verordnung (EU) 2016/679** gibt und gegebenenfalls die Bedingungen des Artikels 9 jener Verordnung sowie des Artikels 5 Absatz 3 der Richtlinie 2002/58/EG erfüllt sind.“*

Art. 5 Abs. 7 DA:

*„…**nur dann** vom Dateninhaber **dem Dritten** bereitgestellt werden, …“*

Verhältnis zwischen Data Act und DSGVO



Rechtsgrundlagen

- Kann Art. 4 Abs. 1 (5Abs. 1) DA gesetzliche Grundlage iSd datenschutzrechtlichen Öffnungsklauseln **Art. 6 Abs. 1 lit. c DS-GVO, Art. 6 Abs. 1 lit. e DS-GVO** und Art. 9 Abs. 2 lit. g DS-GVO (Erforderlichkeit aus erheblichem öffentlichen Interesse) sein?

- Umkehrschluss ErwG 7 und Art. 4 Abs. 12 DA

  (weiteres Problem ePrivacy)

- Aber: **Implizite Einwilligung**, wenn Nutzer = betroffene Person

Rollenverteilung

- Dateninhaber – Verantwortlicher / Auftragsverarbeiter?
  - Bereitstellung der Daten an den Nutzer als Auftragsverarbeitung?
    - Erw.Gr. 22 S. 4 DA Auftragsverarbeiter kein Dateninhaber
    - Aber grds denkbar, wenn gesonderter Verarbeitungsschritt der Bereitstellung
    - Weisungsgebundenheit möglich?
- Nutzer Art. 2 Nr. 12 DA – Betroffene Person
- Dritte – Betroffene Person – Verantwortlicher?

„Es ist kompliziert?“

- Nutzer ist **nicht identisch** mit der betroffenen Person
- DA als RGL? **-> Art. 4 Abs. 12 / Art. 5 Abs. 7**
- Erw.Gr. 7 S.10 DA:

*„Handelt es sich bei dem Nutzer **nicht** um die betroffene Person, so bietet die vorliegende Verordnung **keine Rechtsgrundlage** für die Gewährung des Zugangs zu personenbezogenen Daten oder für deren Bereitstellung an Dritte und sollte nicht so verstanden werden, dass sie dem Dateninhaber ein neues Recht auf die Nutzung personenbezogener Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert wurden, verleiht.“*

- **Art. 6 Abs. 1 lit. c) -**

Einwilligung

- Kein direkter Kommunikationskanal Dateninhaber – Betroffener
- Einholung durch den Nutzer?
- Beweislast aber beim Dateninhaber – Prüfung der Einwilligung?
- Vertragliche Absicherung Dateninhaber – Nutzer?

Vertrag

- Vertrag mit der betroffenen Person erforderlich
- Möglich: Vertrag zwischen Nutzer und Betroffenem
  - Datenübermittlung muss zur Vertragserfüllung erforderlich sein
  - Keine Umgehung des Einwilligungserfordernisses
  - Selbständige Prüfung durch den Dateninhaber erforderlich

Berechtigtes Interesse

1. Stufe: Berechtigtes Interesse

- Erfüllung der gesetzlichen Bereitstellungsverpflichtung aus Art. 3,4 bzw. 5 DA
- Widerspricht nicht den Ausführungen in Erw.Gr. 7
- Grundsätzlich weit auszulegen – Grenze: Gesetzl. Verbote zB. GeschGehG
- Interessen Dritter (auch des Nutzers, zB. Flottenmanagement)

2. Stufe: Erforderlichkeit

- Zweck der Verarbeitung auch durch andere, weniger invasive Mittel erreichbar?
- Zweckbindung / Datenminimierung
- Grds. Erfüllung einer gesetzlichen Pflicht -> **Aber:** Wie?

Berechtigtes Interesse

3. Stufe: Interessensabwägung

- Welche pbD sind betroffen? („Sensible Daten“ – z.B. Standortdaten)
- Kontext der Datenverarbeitung? (z.B. betrieblich/privat)
- Verknüpfung möglich? Durch den Nutzer?
- Mögliche Weiterverarbeitung durch den Nutzer bekannt -> rechtmäßig?
- Auswirkungen auf den Betroffenen
- **Vernünftige Erwartungen des Betroffenen?**
  - Gesetzlich geregelter Vorgang? -> Aber gerade ja keine RGL?
  - Erfüllung der Informationspflichten -> Art. 13/14 ; Art. 3 Abs. 2 Abs. 3 DA

Kernkonflikt

- Saubere Prüfung der Rechtsgrundlage erforderlich
- Option Verarbeitung einfach nicht durchzuführen gibt es nicht
- <u>Doppeltes Risiko:</u>
  - Datenzugang gewährt, in der Annahme kein pB -> Verstoß gegen Art. 5 Abs. 1 DSGVO
  - Datenzugang gewährt, obwohl keine RGL -> Verstoß Art. 5 Abs. 1 DSGVO
  - Datenzugang verweigert, obwohl nach DSGVO möglich -> Verstoß DA

- Nachweispflicht: Verantwortlicher / Dateninhaber

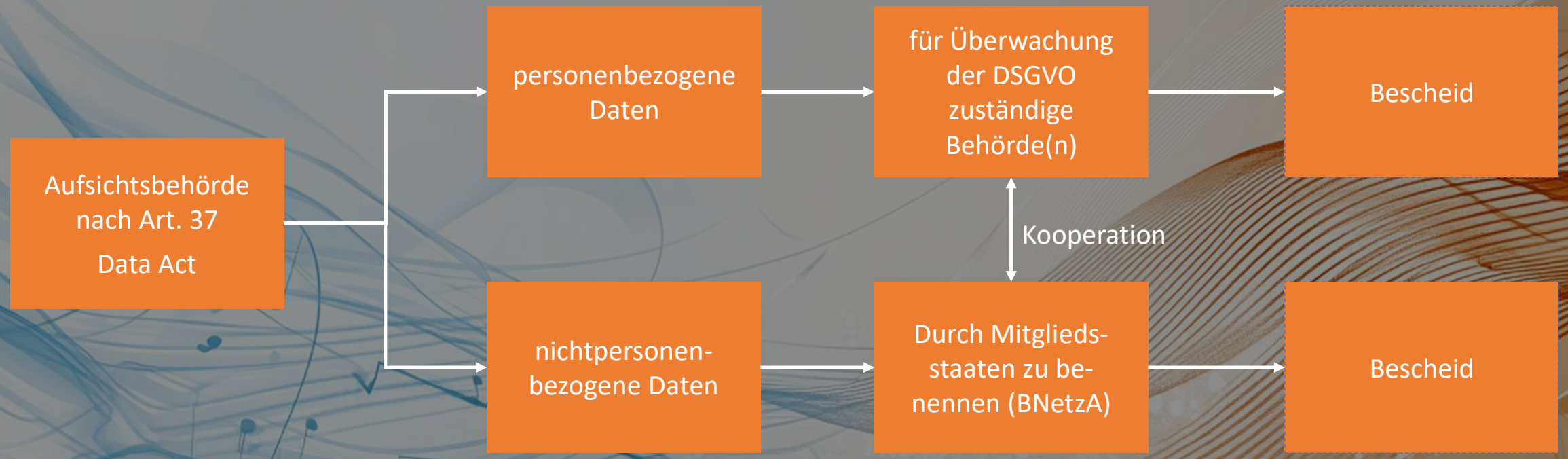
Lösungsansätze?

- Datenmanagement – pbD ja oder nein?
- Vermeidung oder Entfernung des Personenbezugs
  - ErwG. 7: Anonymisierung – Pflicht bei öffentl. Stellen Art. 18 Abs. 4 DA
  - Technische Gestaltung -> Welche Daten werden generiert?
- ErwG 21 S. 4:
  - *„Hersteller oder Entwickler eines vernetzten Produkts, das in der Regel von **mehreren** Personen verwendet wird, sollten die erforderlichen Mechanismen einrichten, die gegebenenfalls die Einrichtung **getrennter Nutzerkonten** für einzelne Personen oder die Nutzung desselben Nutzerkontos durch mehrere Personen ermöglichen.“*
  - Zwang zum Nutzerkonto? -> Art.4 Abs. 5 DA
  - Nutzerkonten auch ohne pbD möglich -> QR-Code/ Barcode
- Hilfestellung und Praxis der zuständigen Behörden

Zuständige Behörden

- Art. 37 Abs. 1, 3 DA: zweigeteilte Aufsicht
- Datenschutzbehörden sind Aufsichtsbehörde nach Data Act bezüglich Schutz personenbezogener Daten
- Grund: Kernfragen der DSGVO!!!

Behördliche Aufsicht nach Data Act



Befugnisse

- Art. 37 Abs. 3 S. 2 DA: Kapitel VI und VII DSGVO finden sinngemäß Anwendung
- **Aufgaben und Befugnisse nach DSGVO** analog, aber auf Pflichten aus dem DA gerichtet
  - Informationen und Dokumente anfordern
  - Technische Prüfungen durchführen
  - Vor-Ort-Ermittlung
  - Abhilfebefugnisse aus DSGVO
  - Anordnung
  - Warnung, Verwarnung
- **Geldbußen** (Art. 40 Abs. 4 DA)
- **Kooperationsverfahren** des EDSA bei grenzüberschreitenden Verfahren (Kapitel VII)

Beschwerderecht

- Datenschutzbehörden sind ab 12.09.2025 für den Teil der pbD betrifft für die Durchsetzung des DA zuständig und bearbeiten auch Beschwerden

- Oftmals keine genaue Abgrenzung zu DSGVO- Beschwerden

Beispiel: Betroffener fordert seine Daten

(Art. 15 DSGVO + Art. 3/4 DA)

- Neu: Datenschutzbehörde setzt Datenzugang B2B durch!

Beispiel: Werkstatt fordert personenbezogene Daten vom Fahrzeughersteller

- Neu? Datenschutzbehörde sucht RGL?

Art. 38 DA – Beschwerderecht

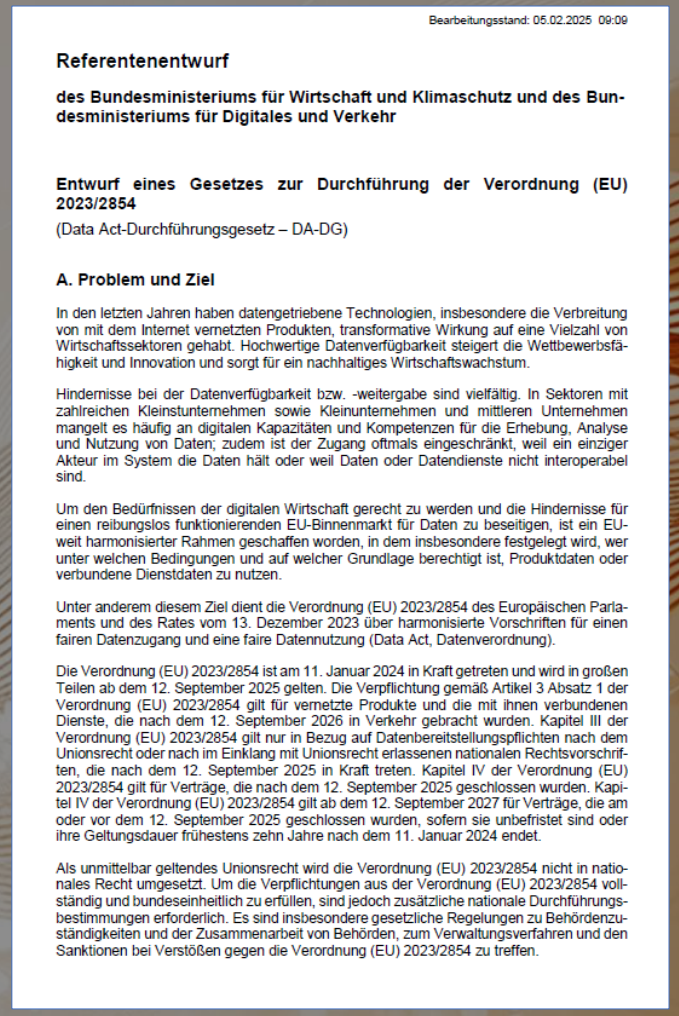
(1) Unbeschadet (…) haben natürliche und juristische Personen das Recht, einzeln oder gegebenenfalls gemeinsam bei der jeweils zuständigen Behörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts (….) (…).

(2) Die zuständige Behörde, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer im Einklang mit dem nationalen Recht über den Stand des Verfahrens und die getroffene Entscheidung

Geplante Umsetzung in Deutschland

- Referentenentwurf vom 5. Februar 2025

- BNetzA als direkte Aufsichtsbehörde - Außenverhältnis
- bindet in Datenschutzfragen BfDI intern ein
- nur BNetzA führt Ermittlungen
- nur BNetzA erlässt Bescheide, berücksichtigt darin die Einschätzung der BfDI
- Landesbehörden nicht vorgesehen, obwohl sie nach DSGVO zuständig sind



Bearbeitungsstand: 05.02.2025 09:09

Referentenentwurf

des Bundesministeriums für Wirtschaft und Klimaschutz und des Bundesministeriums für Digitales und Verkehr

Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854

(Data Act-Durchführungsgesetz – DA-DG)

A. Problem und Ziel

In den letzten Jahren haben datengetriebene Technologien, insbesondere die Verbreitung von mit dem Internet vernetzten Produkten, transformative Wirkung auf eine Vielzahl von Wirtschaftssektoren gehabt. Hochwertige Datenverfügbarkeit steigert die Wettbewerbsfähigkeit und Innovation und sorgt für ein nachhaltiges Wirtschaftswachstum.

Hindernisse bei der Datenverfügbarkeit bzw. -weitergabe sind vielfältig. In Sektoren mit zahlreichen Kleinstunternehmen sowie Kleinunternehmen und mittleren Unternehmen mangelt es häufig an digitalen Kapazitäten und Kompetenzen für die Erhebung, Analyse und Nutzung von Daten; zudem ist der Zugang oftmals eingeschränkt, weil ein einziger Akteur im System die Daten hält oder weil Daten oder Datendienste nicht interoperabel sind.

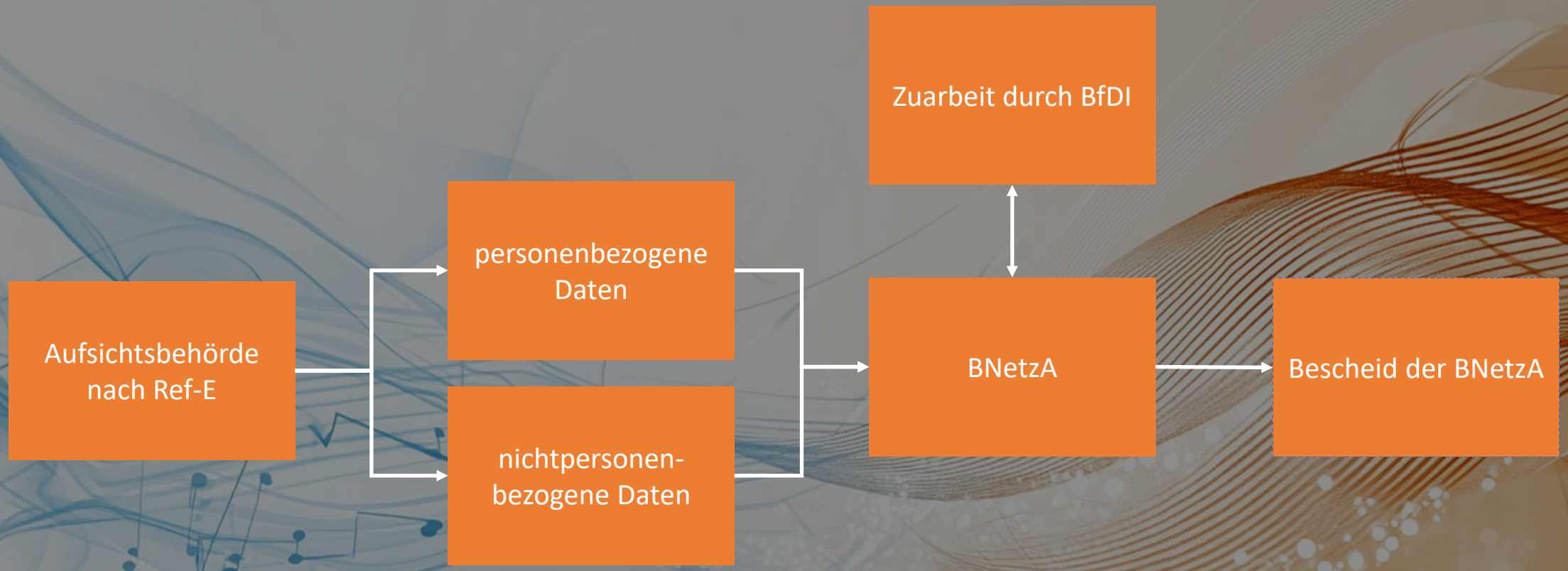
Um den Bedürfnissen der digitalen Wirtschaft gerecht zu werden und die Hindernisse für einen reibungslos funktionierenden EU-Binnenmarkt für Daten zu beseitigen, ist ein EU-weit harmonisierter Rahmen geschaffen worden, in dem insbesondere festgelegt wird, wer unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, Produktdaten oder verbundene Dienstdaten zu nutzen.

Unter anderem diesem Ziel dient die Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act, Datenverordnung).

Die Verordnung (EU) 2023/2854 ist am 11. Januar 2024 in Kraft getreten und wird in großen Teilen ab dem 12. September 2025 gelten. Die Verpflichtung gemäß Artikel 3 Absatz 1 der Verordnung (EU) 2023/2854 gilt für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12. September 2026 in Verkehr gebracht wurden. Kapitel III der Verordnung (EU) 2023/2854 gilt nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, die nach dem 12. September 2025 in Kraft treten. Kapitel IV der Verordnung (EU) 2023/2854 gilt für Verträge, die nach dem 12. September 2025 geschlossen wurden. Kapitel IV der Verordnung (EU) 2023/2854 gilt ab dem 12. September 2027 für Verträge, die am oder vor dem 12. September 2025 geschlossen wurden, sofern sie unbefristet sind oder ihre Geltungsdauer frühestens zehn Jahre nach dem 11. Januar 2024 endet.

Als unmittelbar geltendes Unionsrecht wird die Verordnung (EU) 2023/2854 nicht in nationales Recht umgesetzt. Um die Verpflichtungen aus der Verordnung (EU) 2023/2854 vollständig und bundeseinheitlich zu erfüllen, sind jedoch zusätzliche nationale Durchführungsbestimmungen erforderlich. Es sind insbesondere gesetzliche Regelungen zu Behördenzuständigkeiten und der Zusammenarbeit von Behörden, zum Verwaltungsverfahren und den Sanktionen bei Verstößen gegen die Verordnung (EU) 2023/2854 zu treffen.

Aufsichtsstruktur nach Referentenentwurf



Kritik am Referentenentwurf

- Offenkundige Verfassungs- und Europarechtswidrigkeit
- kein Gleichlauf in der Datenschutzaufsicht nach DSGVO und Data Act
- BfDI werden die Befugnisse nach Data Act entzogen
- Bundesaufsicht auch über öffentliche Stellen der Länder
- DA sieht Kohärenzverfahren des EDSA vor

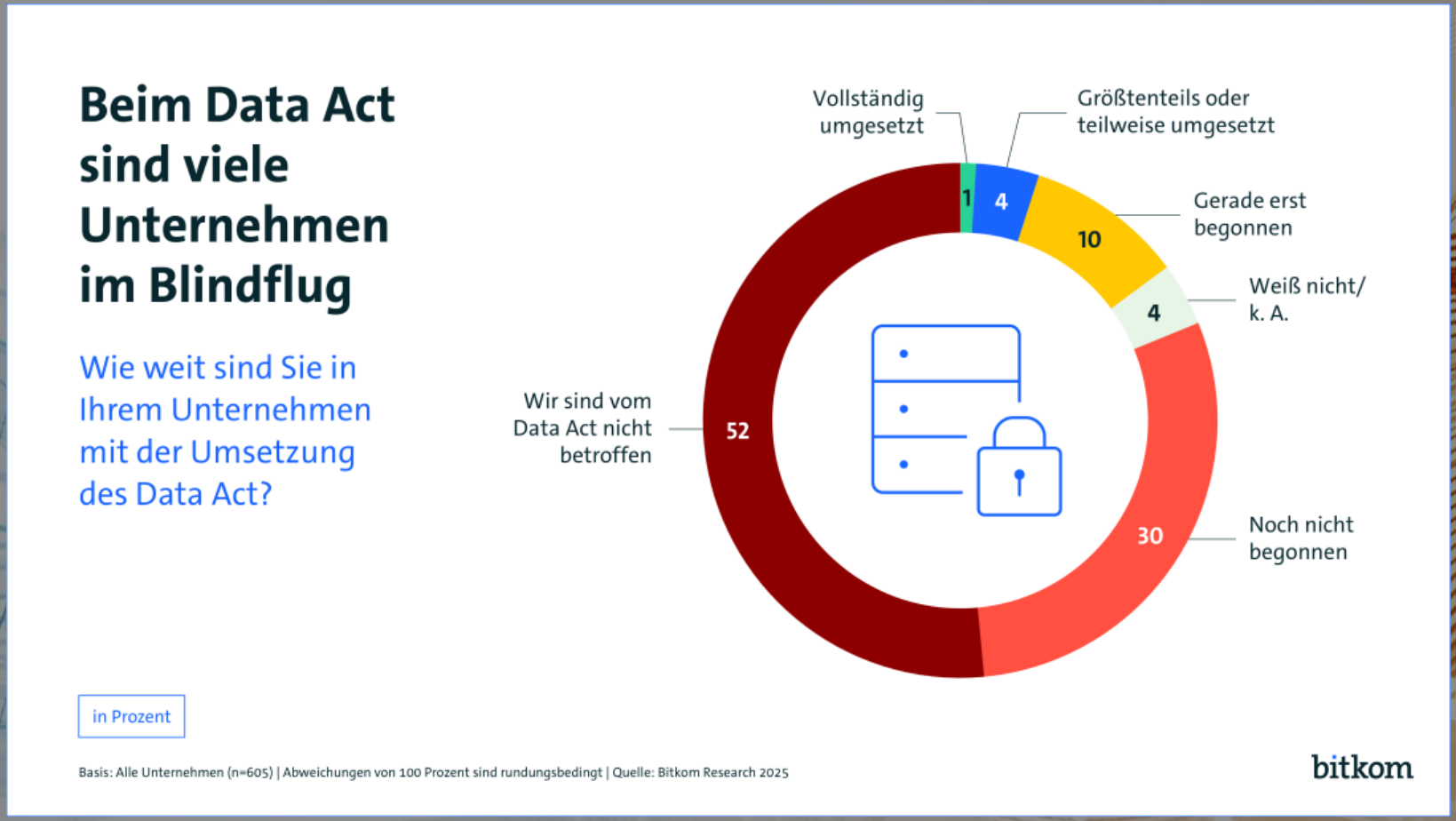
- Rein deutsche Diskussion!
- Noch kein Gesetz…

Folgen des fehlenden Durchführungsgesetzes

- Datenschutzbehörden automatisch zuständig für personenbezogene Daten
- Art. 37 Abs. 3 DA wirkt direkt, keine nationale Umsetzung erforderlich
- Aufgaben und Befugnisse direkt aus Art. 37 Abs. 3 DA i.V.m. DSGVO
- zunächst keine Aufsicht für nichtpersonenbezogene Daten
- Keine rückwirkenden Geldbußen möglich, erst ab Geltungsbeginn Durchführungsgesetz

- Zugangsansprüche können zivilrechtlich verfolgt werden

Folgen des fehlenden Durchführungsgesetzes



https://www.bitkom.org/Presse/Presseinformation/Data-Act-Kaum-Unternehmen-vorbereitet#_

Zeit für Ihre Fragen!

Carolin Loy

Bayerisches Landesamt für Datenschutzaufsicht

Promenade 18

91522 Ansbach

E-Mail: carolin.loy@lda.bayern.de

https://www.lda.bayern.de