

Der Data Act: Wie die EU die europäische Datenwirtschaft nach vorne bringen möchte

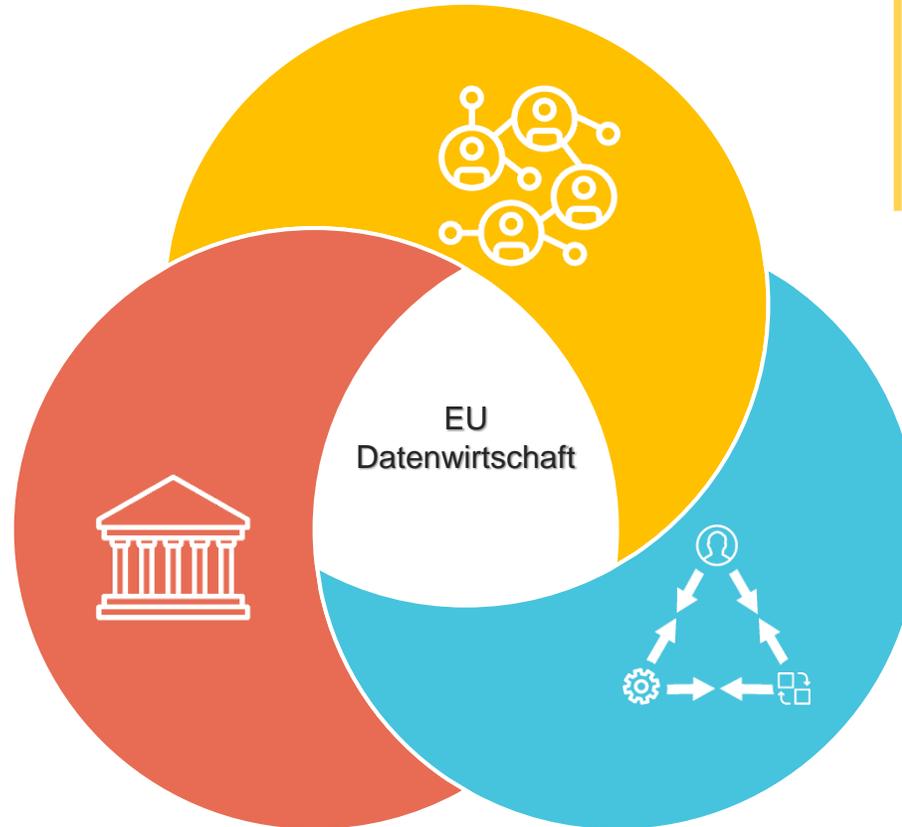
Sören Schneider

Referent, DG CNECT, Referat G.1
(Datenpolitik und –innovation)

Webinar der IHK für München und Oberbayern, 3. Juli 2025

Europäische Datenstrategie (2020)

Gesetzgebung
Den Schatz an Industriedaten in Europa heben und eine robuste sowie faire datengetriebene Wirtschaft schaffen



Bereitstellung von Datenräumen

Unterstützung und Einrichtung EU-weiter gemeinsamer und interoperabler Datenräume für den freiwilligen Datenaustausch in strategischen Sektoren



Fördermittel

Stärkung der europäischen Dateninfrastruktur und -technologien



The bigger vision: a European Single Market for Data

European data strategy, Feb 2020

Horizontal Data Legislation

Data Act

Data Governance Act

Open Data Directive

Free Flow of Data Regulation

GDPR

...

Common European Data Spaces



Health



Manufact.



Agriculture



Finance



Mobility



Green Deal



Energy



Public Admin.



Skills



R&I (EOSC)



Tourism



Cultural heritage



Media



Language

High Value Datasets from public sector

European Data Innovation Board

- Prioritisation of cross-sectoral interoperability standards
- Facilitate the sharing of good practices

Data Spaces Support Centre

- Coordination and support of data space projects
- Development of blueprint, glossary, etc.

Technical Infrastructure

Standards / Interoperability

Digital identity (eIDAS)

Smart Middleware Platform (Simpl)

High-Performance Computing

Testing and Experimentation Facilities

Warum ein Data Act?

- Das Potenzial von Daten, insbesondere von Industriedaten, wird **nicht in vollem Umfang ausgeschöpft**
- Unklarheit darüber, **wer** unter **welchen Bedingungen** aus **welchen Daten** Nutzen ziehen kann
- Gefahr der **Fragmentierung** des EU-Marktes, die zu höheren Compliance-Kosten führt



Der Data Act ist ein **game-changer** für den Zugang und die Nutzung von Daten



Abwägung der Interessen derjenigen, die in Datentechnologien investieren, und derjenigen, die zur Datenerzeugung beitragen



Data Act

Verordnung (EU) 2023/2854 vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung

Besserer Zugang zu **IoT Daten**

Regeln für IoT-Daten bestimmen auch den Datenaustausch in anderen Sektoren



Verhinderung **missbräuchlicher Vertragsklauseln** beim B2B Datenaustausch



Unternehmensdaten für das Allgemeinwohl verfügbar machen (B2G)



Einfacher zwischen Clouddiensten **wechseln**

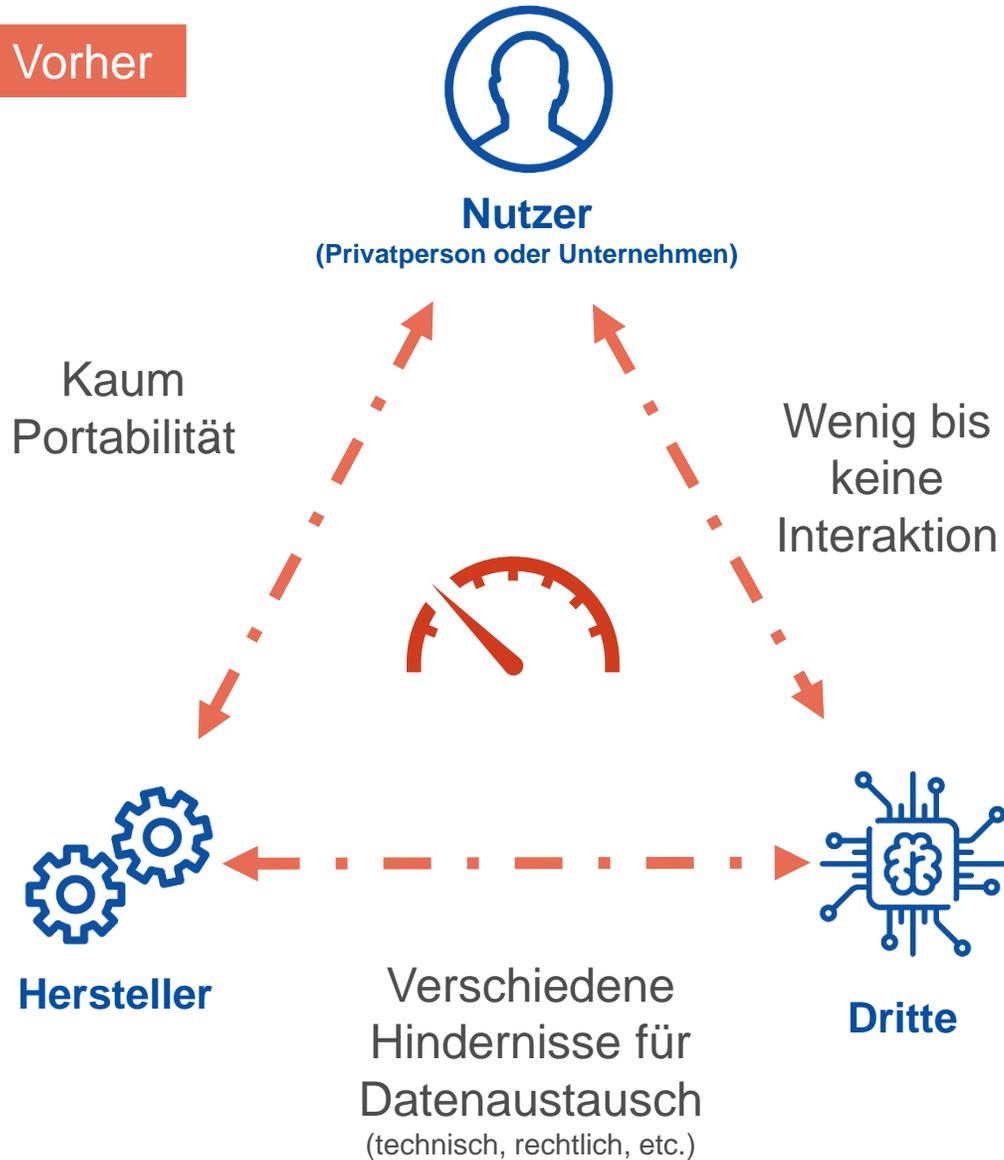


Förderung von Datenflüssen durch **Standards** und **Interoperabilität**, insb. für Datenräume

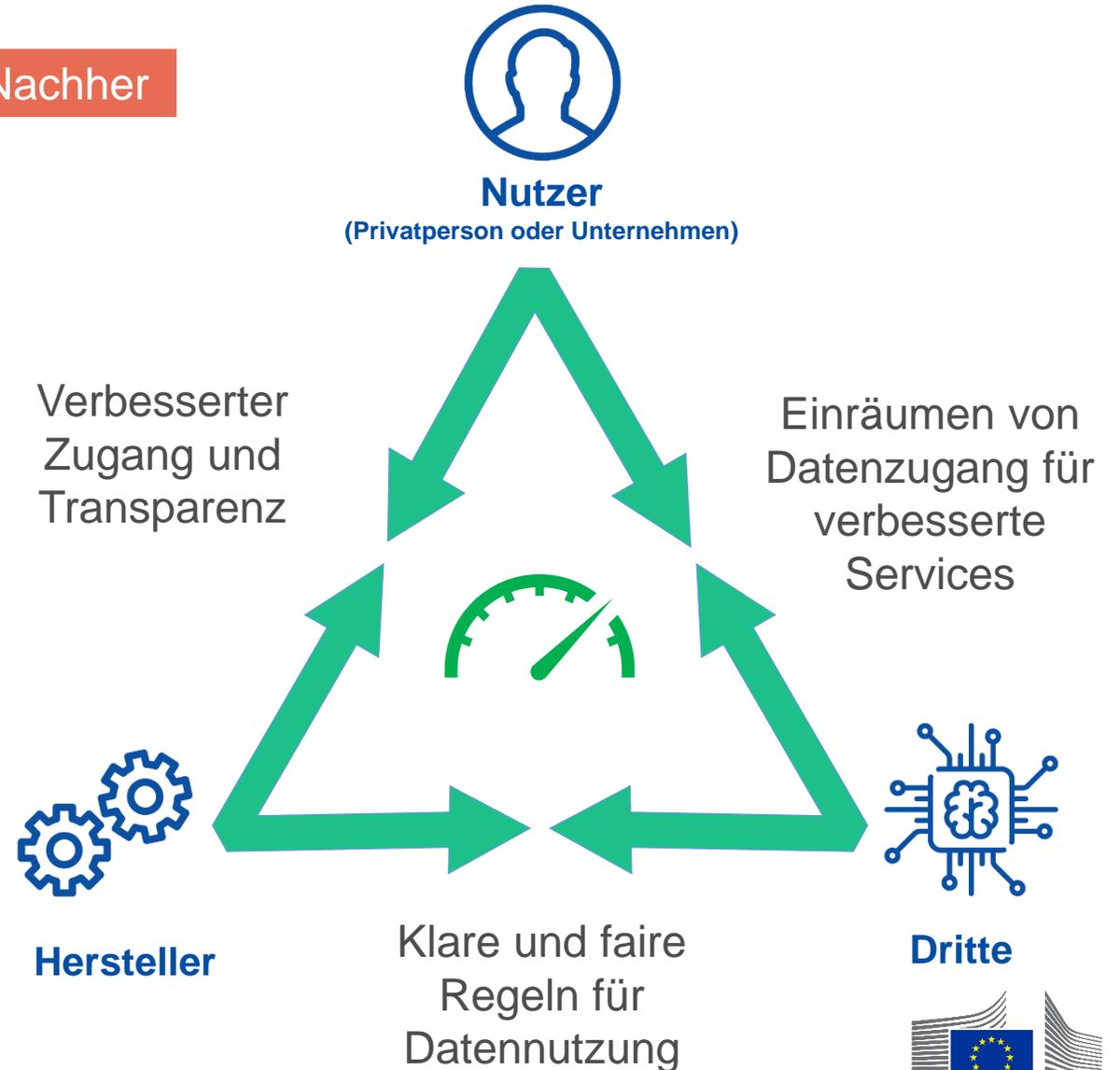


Nutzung von IoT-Daten (B2B & B2C)

Vorher



Nachher



Kapitel II: Besserer Zugang zu Daten

- Kernidee: Nutzer von vernetzten Produkten (v.a. IoT-Objekte) haben das Recht auf Zugang zu und Weitergabe von Daten, die sie durch die Nutzung dieser Objekte erzeugen und die bei einem Dateninhaber «ohne Weiteres verfügbar» sind
 - Nutzer ist, wer eine zivilrechtliche Beziehung zu einem Objekt hat; reiner Besitz reicht nicht.
 - Erfasst sind Privatpersonen (B2C) und Unternehmen (B2B)
 - (+) Eigentümer, Mieter etc.
 - (-) Rein tatsächliche Nutzung ohne Rechtsbeziehung (z.B. Benutzer von Aufzügen oder Rolltreppen)



Kapitel II: Produkte und verbundene Dienste („Related Services“)

- Erfasst sind vernetzte Produkte (= Hardware) & Steuerapps oder Web Services (= related service)
- Kapitel II Data Act will Daten aus Hardware erfassen, die heute in der Lage ist, solche Daten nach außen zu übermitteln („designed to be retrievable“).
- Die Daten können durch verbaute Sensoren oder durch die Interaktion mit dem Nutzer (on-device interfaces - Knöpfe, Touchscreen) oder durch die Nutzung von Steuersoftware als App oder Web Service (=„related service“) entstehen („digitisation of user actions“)



Kapitel II: Welche Daten sind (nicht) erfasst?

- Erwägungsgrund 15:
 - (+) – Rohdaten (z.B. Sensordaten) und aufbereitete Daten („raw and pre-processed“)
 - (+) – Metadaten
 - (+) – ohne weiteres verfügbare Daten („readily available“)
 - (-) – abgeleitete Daten („inferred or derived data“), Inhalte (→ Copyright!)
 - (-) – Daten, die nicht aus dem Produkt übermittelt werden können
- Hintergrund:
 - Anreize schützen, in innovative Datenprodukte zu investieren
 - Level-playing-field zwischen Dateninhaber und Nutzer/Dritten herstellen





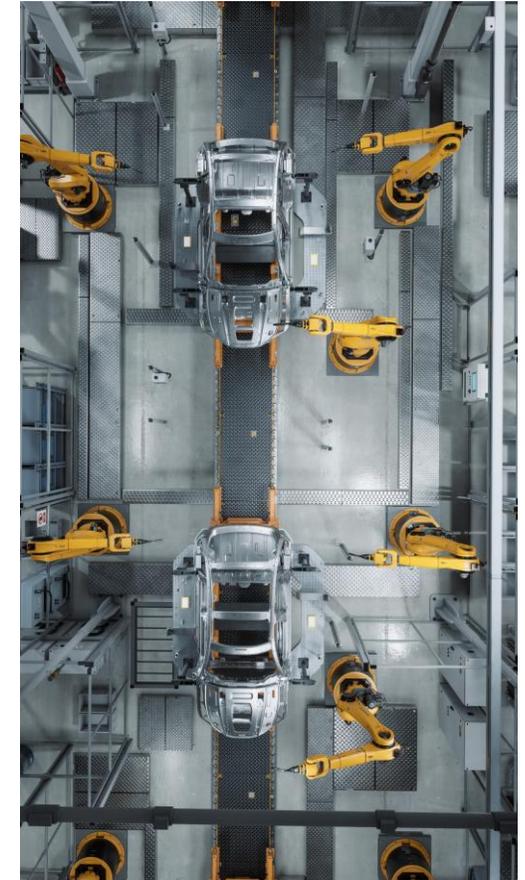
Grundregeln

- **Dateninhaber** (in der Regel die Hersteller) müssen:
 - **Transparenzpflichten erfüllen.** Nutzer müssen über die vom Produkt oder verbundenen Dienst generierte Daten und die Zugangsmöglichkeit informiert werden. Bsp.: Verpackung, QR-Code
 - **Einen einfachen und kostenlosen Datenzugang für Nutzer sicherstellen.** Bsp: direkt über das Produktinterface oder indirekt über einen online Nutzeraccount.
 - Auf Verlangen des Nutzers **Daten an Dritte weitergeben** (Vergütung bei Dritten möglich).
 - **Geschäftsgeheimnisse** identifizieren und sich mit Nutzern/Dritten auf geeignete Schutzmaßnahmen einigen
 - dürfen **nicht-personenbezogene** Daten nur mit vertragl. **Einverständnis** des Nutzers für sich nutzen
- Ausn: **Klein- und Kleinstunternehmen** (< 50 Mitarbeitende und Jahresumsatz < 10 Mio. EUR), es sei denn
 - größeres Partner- oder verbundenes Unternehmen;
 - als Unterauftragnehmer mit Herstellung/Konzeption beauftragt
- **Dritte**, die Daten empfangen:
 - Müssen **sich mit dem Dateninhaber** auf Schutzmaßnahmen zur Bewahrung von Vertraulichkeit und Geschäftsgeheimnissen **einigen.**
 - Dürfen ohne Einverständnis des Nutzers **keine Daten mit anderen teilen.**
 - Dürfen keine **DMA gatekeeper** sein.
 - Dürfen mithilfe der empfangenen Daten **keine konkurrierenden Produkte entwickeln.**
 - Dürfen Verbraucher-Nutzer nicht daran hindern, **die erhaltenen Daten anderen Parteien bereitzustellen.**



Pflicht zum Redesign von Produkten?

- Art. 3 Abs. 1: Hersteller stellen einen direkten Datenzugang sicher – aber nur soweit:
 1. relevant, und
 2. technisch durchführbar
- Auslegung:
 - Keine unbedingte Pflicht
 - Ermessen über das Design des vernetzten Produkts
 - Hersteller haben die Wahl, Datenzugang direkt oder indirekt zu gewähren
- Warum das wichtig ist:
 - **Keine Pflicht zum Redesign von Produkten**
 - Nicht alle Daten müssen “by design” direkt zugänglich sein
 - Transparenzregeln gelten – Nutzer müssen wissen, welche Daten und wie der Zugang funktioniert



Schutz von personenbezogenen Daten und Privatsphäre

Der Data Act **ändert** die Unionsgesetze zum Schutz von personenbezogenen Daten und der Privatsphäre **nicht**, sondern **ergänzt** sie lediglich

→ **Jede Verarbeitung** personenbezogener Daten gemäß dem Data Act muss die EU-Vorgaben zum Datenschutz beachten, inkl. des Erfordernisses einer **Rechtsgrundlage** zur Datenverarbeitung nach **Art.6 DSGVO**



‘Notfall-Handbremsen’



Geschäftsgeheimnis-Handbremse: Inhaber von Geschäftsgeheimnissen können die Anfrage zum Datenzugang oder zur Datenweitergabe **ablehnen**, wenn die Preisgabe mit hoher Wahrscheinlichkeit zu einem **schweren wirtschaftlichen Schaden** führt und dies auf Grundlage **objektiver und nachvollziehbarer Faktoren** begründet wird.

Sicherheits-Handbremse: Dateninhaber können Anfragen wegen Sicherheitsbedenken nur **unter besonderen Umständen** und im **Einzelfall** ablehnen.

Schutzmaßnahmen gegen Missbrauch:

- Dateninhaber müssen die **Notwendigkeit** der Handbremsen belegen
- Die zuständigen Behörden müssen über die Aktivierung der Handbremsen **benachrichtigt** werden
- Beschwerde- und Streitbeilegungsverfahren
- Evaluation durch Kommission (Art. 49)



Kapitel III: Bedingungen des Datenzugangs gemäß Kapitel II bei B2B



Bereitstellung zu FRAND Bedingungen
(fair, reasonable and non-discriminatory)
Gewährleistet Fairness beim Datenaustausch



Dateninhaber und Datenempfänger
können angemessene Vergütung
vereinbaren
*Anreize zur Datenerhebung
bewahren*

Vergütung ist für KMUs auf Kosten der
Datenbereitstellung gedeckelt
KMUs schützen

Sektor-spezifisches Recht kann
Sonderregeln zu Vergütung enthalten
Schafft Flexibilität

Grundregel: falls rechtliche
Verpflichtung zur Bereitstellung von
Daten, *dann:*

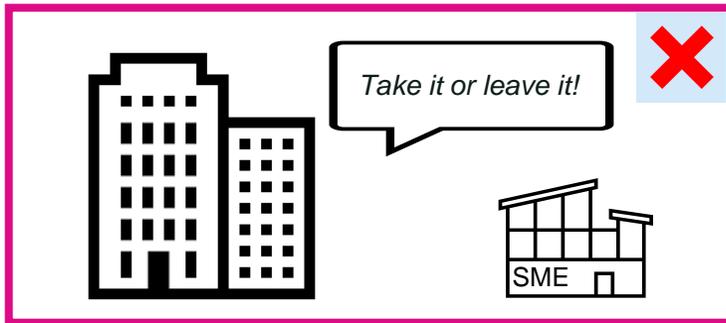


Staatlich zertifizierte
Streitbeilegungsstellen können
Parteien bei Streitigkeiten
unterstützen

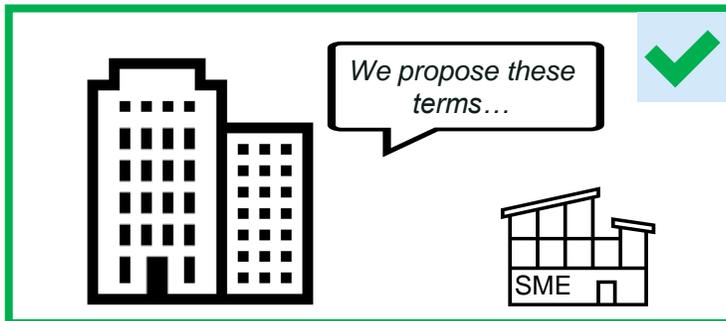
Kapitel IV: Missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung (B2B)

Einseitig auferlegte missbräuchliche Vertragsklauseln sind für Unternehmen nicht bindend

Von...



...zu echten Verhandlungen.



Allgemeine Regel zur Missbräuchlichkeit

grobe Abweichung von der guten Geschäftspraxis bei Datenzugang/-nutzung oder Verstoß gegen Treu und Glauben

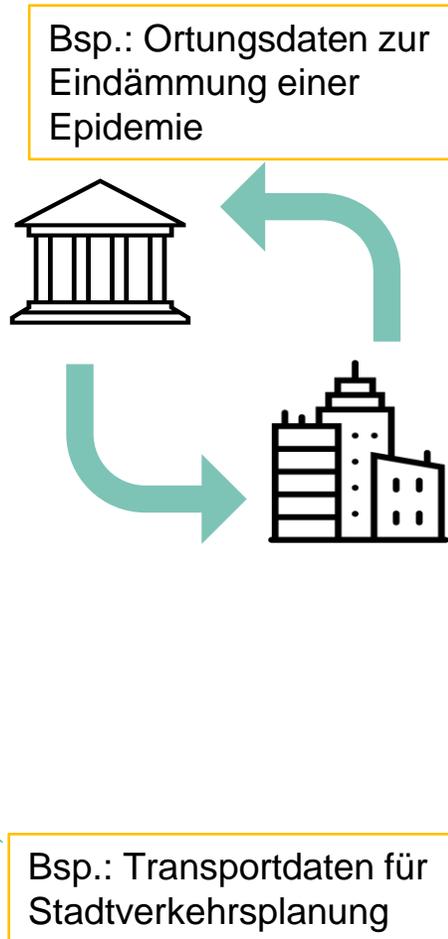
Katalog von Klauseln, die unwiderleglich (Art. 13 Abs. 4) /widerleglich (Art. 13 Abs. 5) als missbräuchlich gelten (Beispiele):

- Ausschluss oder die Beschränkung der Haftung des Verwenders für vorsätzliche und grob fahrlässige Handlungen.
- Ausschluss von Rechtsbehelfen der anderen Vertragspartei bei Nichterfüllung oder Verletzung von Vertragspflichten
- Hinderung der anderen Vertragspartei, den Vertrag innerhalb angemessener Frist zu kündigen

Kapitel V: B2G – Mechanismus für den Zugang zu Unternehmensdaten

Öffentliche Stellen können bei außergewöhnlicher Notwendigkeit Daten anfordern:

- zur Bewältigung eines öffentlichen Notstands (jegliche Daten, inkl. von Klein(st)unternehmen)
- wo Daten zur Aufgabenerfüllung im öffentlichen Interesse erforderlich sind und die Daten sonst nicht verfügbar sind (nur nicht-personenbezogene Daten)



Unternehmen müssen Daten verfügbar machen, jedoch:

- Zweck und Zeitraum müssen klar in der Datenanfrage definiert sein
- nur gegen angemessene Vergütung (außer
 - 1] die Anfrage dient der Notstandsbewältigung und das angefragte Unternehmen ist kein Klein(st)unternehmen, oder
 - 2] nat. Statistikbehörden ist Datenerwerb rechtlich untersagt)

Die geteilten Daten werden nur für einen bestimmten Zweck genutzt und nach Nutzung gelöscht (Ausn.: Aufbewahrung ist gesetzlich vorgeschrieben)

Kapitel VI: Hindernisse beim Wechsel von Cloudanbietern beseitigen



Kostenfreier Wechsel

- Keine Extragebühren
- Keine "Datenextraktions entgelte"



Schneller Wechsel

- Vorhersehbarer Zeitplan
- Vorgaben zu Kündigungsfrist/ Übergangsphase



Reibungsloser Wechsel

- Technische Hindernisse beseitigen

Kapitel VII: Internationale Aspekte

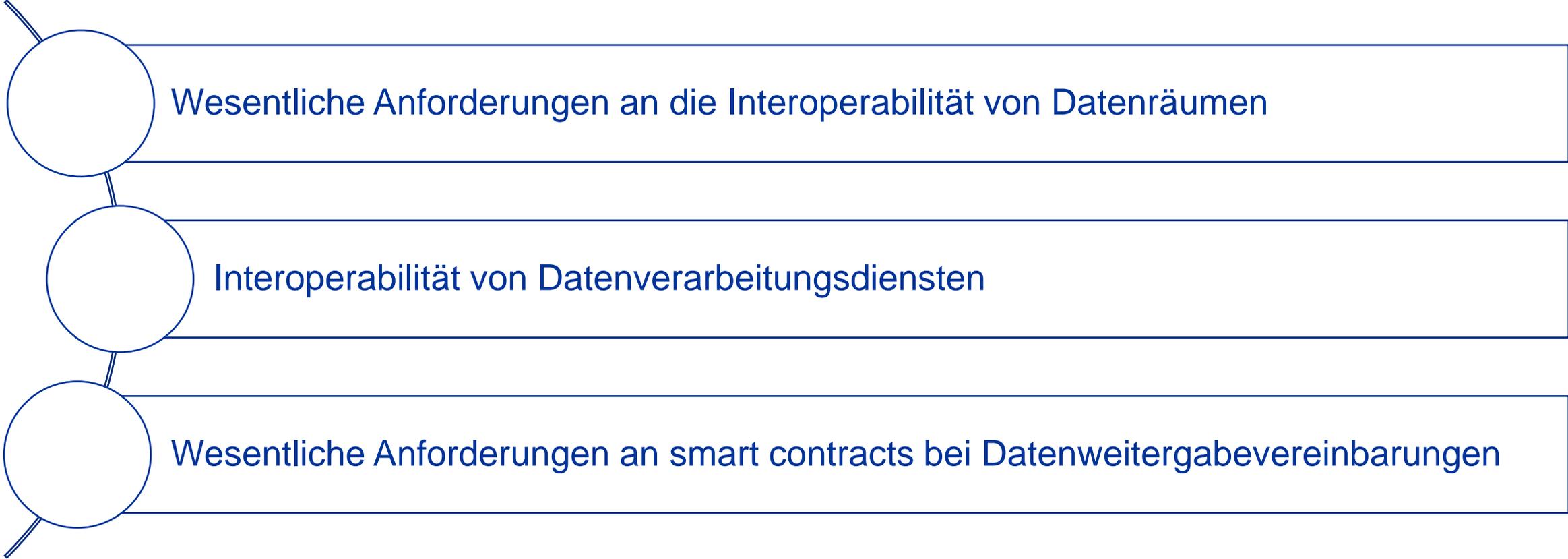
Europäische Daten schützen und EU-Regeln und -Werte respektieren

Anbieter von Datenverarbeitungsdiensten treffen alle **angemessenen technischen, organisatorischen und rechtlichen Maßnahmen**, einschließlich Verträgen, um den unrechtmäßigen staatlichen Zugang zu und die staatliche Übermittlung von in der Union gespeicherten nicht-personenbezogenen Daten im internationalen Umfeld und durch Drittländer zu verhindern

Verfahrensgarantien für die Vollstreckbarkeit von Gerichts- oder Verwaltungsentscheidungen aus Drittländern.



Kapitel VIII: Interoperabilität



Wesentliche Anforderungen an die Interoperabilität von Datenräumen

Interoperabilität von Datenverarbeitungsdiensten

Wesentliche Anforderungen an smart contracts bei Datenweitergabevereinbarungen

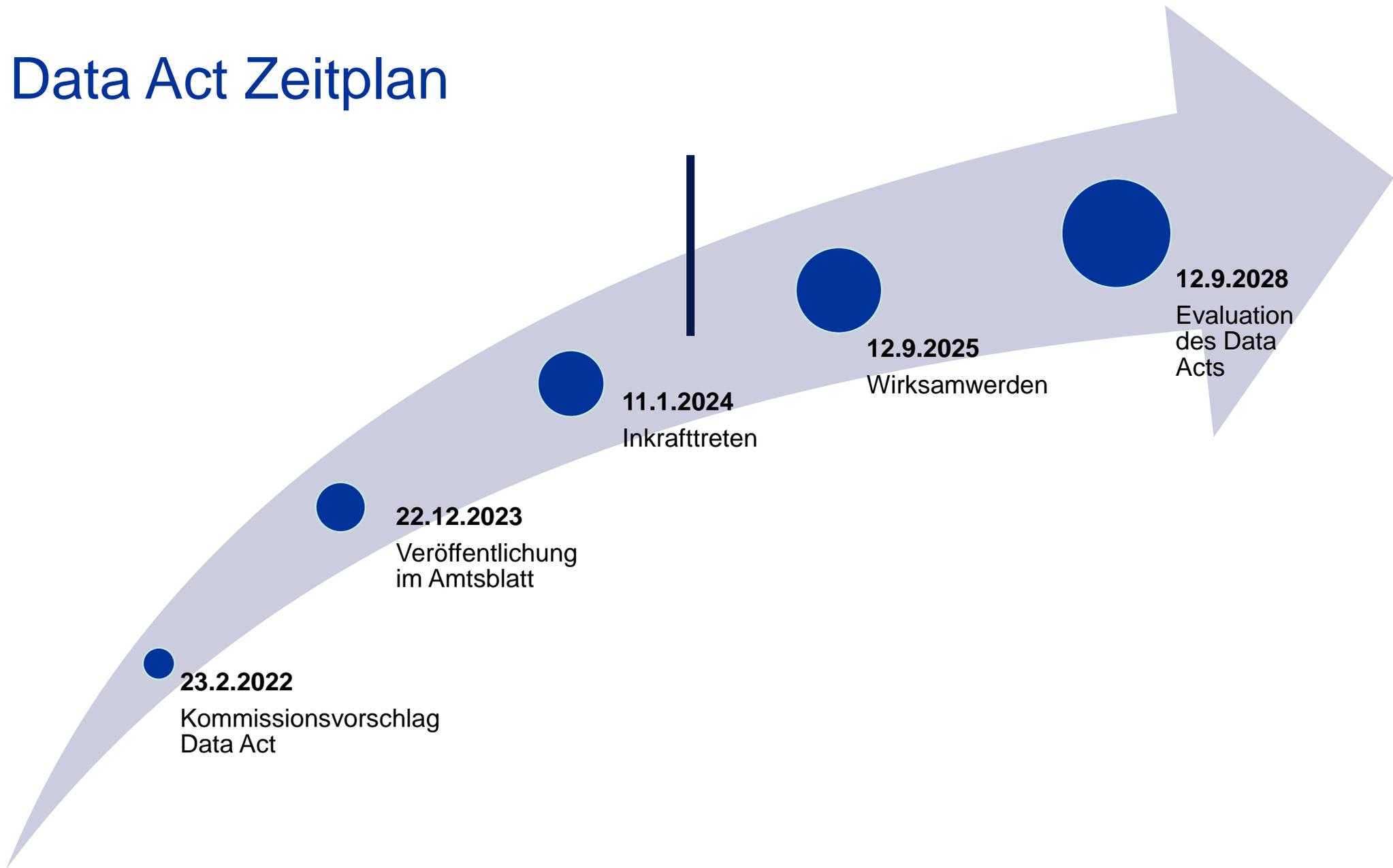
Kapitel IX: Durchsetzung

Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden für die Anwendung und Durchsetzung des Data Acts

- ‘**Datenkoordinatoren**’ agieren als “single point of contact”
- Es kann sich um bereits vorhandene Stellen und Strukturen handeln
- Befugnisse der **Datenschutzbeauftragten** sowie der **sektorspezifischen Behörden** bleiben **unberührt**



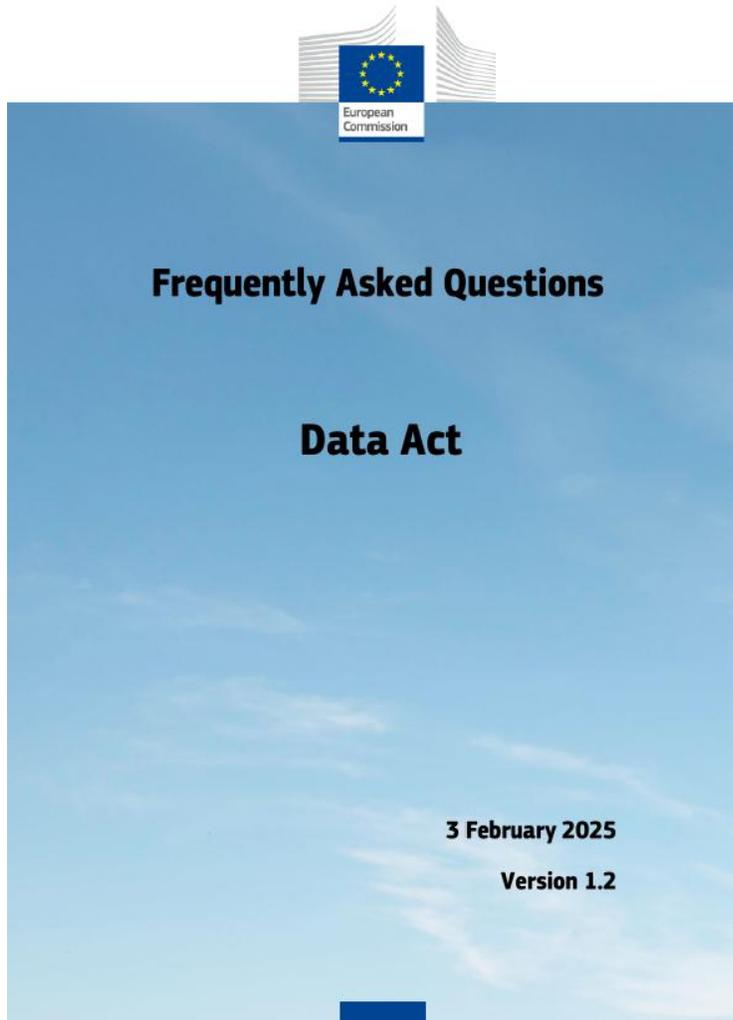
Data Act Zeitplan



Wie unterstützt die Kommission bei der Umsetzung?



Frequently Asked Questions

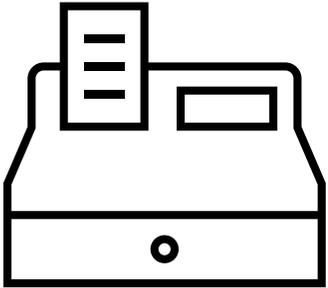


**Unverbindliche Mustervertragsklauseln für B2B Datenaustausch
und Standardvertragsklauseln für Cloud-Computing-Verträge -
*Herbst 2025***



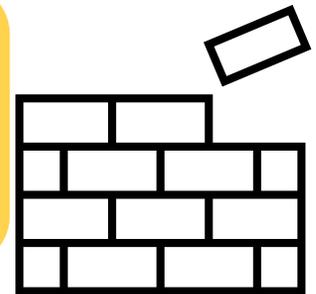
Leitlinien und Standards

Leitlinien für die Berechnung einer angemessenen
Gegenleistung – *Herbst 2025*



Leitlinien für fahrzeuggenerierte Daten – *Herbst 2025*

Interoperabilitäts- und Standardisierungsbemühungen –
Erarbeitung eines Standards für einen “**European Trusted Data
Framework**”



Was wird der Data Act ändern?



Harmonisierte Regeln für Datenzugang und –nutzung, um den **EU Industriedatenschutz zu heben**



Neue datenbasierte Geschäftsmodelle



Privatpersonen und Unternehmen ermächtigen, vernetzte Produkte und verbundene Dienste zu nutzen



Mehr Transparenz und Kontrolle über Daten



Verbesserung öffentlicher Dienstleistungen, inkl. Notstandsbewältigung



Bessere und effizientere Verwaltung und Politik



Wechsel für Cloudnutzer vereinfachen durch Interoperabilität



Ein interoperabler Markt für Cloud-/Edgedienste mit vielen Anbietern

Zusammenfassung:

- Der **Data Act** bringt Verpflichtungen, aber auch **viele Chancen** mit sich.
- **Ausgewogenheit** zwischen Datenzugang zur Schaffung von **Innovation** und dem **Schutz** legitimer Interessen von Unternehmen.
- Alle Elemente der EU Datenstrategie sind im Spiel: nun liegt der **Fokus** auf der **Umsetzung**.



Danke sehr!



© European Union 2025

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

