

CLARITY LAYER
DATA STRATEGY & GOVERNANCE

Der EU Data Act Zusammenfassung

www.clarity-layer.com

Inhalt

- 01 Was ist der EU Data Act?
- 02 Wer ist betroffen?
- 03 Zentrale Pflichten und Rechte
- 04 Durchsetzung und Sanktionen
- 05 Kurzfassung



Was ist der EU Data Act?

Der EU Data Act legt Regeln dafür fest, wie Daten aus vernetzten Produkten und zugehörigen digitalen Diensten innerhalb der EU geteilt, zugänglich gemacht und geschützt werden.

Ziel ist es, Daten fair zugänglich, sicher teilbar und innovationsfördernd zu nutzen, ohne dass große Marktteilnehmer andere durch Abschottung ausschließen.

Wer ist betroffen?

Gruppe	Rolle	Beispiele
Hersteller vernetzter Produkte	Stellen Geräte her, die Daten erzeugen oder erfassen.	Smart Cars, Traktoren, medizinische Geräte, IoT-Sensoren, Smart-Home-Technologien
Anbieter verbundener Dienste	Bieten digitale Services an, die mit diesen Produkten verbunden sind.	Fahrzeugflotten-Apps, Fitness-Dashboards, industrielle Monitoring-Tools
Nutzer (Personen oder Unternehmen)	Nutzen die Produkte und erzeugen dadurch Daten.	Ein Landwirt mit einem vernetzten Traktor, ein Fahrer eines smarten E-Autos
Dateninhaber	Kontrollieren oder verwalten den Zugriff auf die Daten.	Ein Automobilhersteller, der Fahrzeugleistungsdaten speichert
Dritte (Datenempfänger)	Erhalten mit Zustimmung Zugriff auf Daten.	Unabhängige Werkstätten, Analytics-Startups, Versicherungen, Forschende
Cloud- und Edge-Service-Anbieter	Speichern und verarbeiten Daten.	AWS, Azure, Google Cloud, lokale Hosting-Anbieter
Öffentliche Stellen	Dürfen Daten nur in Ausnahmefällen anfordern, etwa bei Notlagen oder im öffentlichen Interesse.	Statistische Ämter, Katastrophenschutzbehörden

Zentrale Pflichten und Rechte

1

Hersteller und Dateninhaber

- Müssen Daten aus vernetzten Produkten einfach und kostenlos für Nutzer bereitstellen
- Müssen Daten sicher und diskriminierungsfrei an vom Nutzer gewählte Dritte weitergeben
- Müssen klare, verständliche Informationen darüber liefern, welche Daten entstehen und wie darauf zugegriffen werden kann
- Müssen Geschäftsgeheimnisse schützen, dürfen diese aber nicht als Vorwand zur Verweigerung des Zugriffs nutzen
- Müssen APIs oder andere technische Schnittstellen für zeitnahen und kontinuierlichen Zugriff bereitstellen

Beispiel:

Ein Automobilhersteller muss Kundinnen und Kunden oder autorisierten Werkstätten Zugriff auf Fahrzeugsensordaten ermöglichen, nicht nur über die eigene App.

Nicht zulässig:

Überhöhte Gebühren oder verzögerter Zugriff für Wettbewerber.

2

Nutzer (Privatpersonen oder Wettbewerber)

- Haben das Recht, auf die von ihren Geräten erzeugten Daten zuzugreifen
- Können anweisen, dass diese Daten an einen Dritten weitergegeben werden (z. B. eine Reparatur- oder Analysefirma)
- Haben Anspruch auf klare Erklärungen, welche Daten erhoben werden und zu welchem Zweck

Beispiel:

Ein Landwirt kann den Traktorenhersteller anweisen, Bodendaten an ein unabhängiges Agritech-Unternehmen zu senden.

Zentrale Pflichten und Rechte

3

Dritte (Datenempfänger)

- Dürfen Daten nur mit Zustimmung des Nutzers erhalten
- Dürfen die Daten ausschließlich für den vereinbarten Zweck verwenden
- Müssen Daten sicher speichern, dürfen sie nicht weiterverkaufen oder ohne Zustimmung zur Identifizierung nutzen
- Müssen Daten löschen, sobald sie nicht mehr benötigt werden

Beispiel:

Eine Werkstatt darf Diagnosedaten zur Reparatur nutzen, aber nicht für Marketing oder zur Weitergabe an Versicherungen.

4

Cloud- und Edge-Service-Anbieter

- Müssen einen einfachen Anbieterwechsel ermöglichen (kein Vendor Lock-in)
- Müssen Datenübertragbarkeit sicherstellen
- Müssen Daten sicher speichern und verarbeiten
- Müssen Daten vor unzulässigem Zugriff durch Nicht-EU-Behörden schützen (außer bei gesetzlicher Verpflichtung)

Beispiel:

Ein Unternehmen kann seine Daten von AWS zu Azure migrieren, ohne versteckte Gebühren oder lange Verzögerungen.

Zentrale Pflichten und Rechte

5

Öffentliche Stellen

- Dürfen Daten nur in Ausnahmefällen anfordern (z. B. Naturkatastrophen, Pandemien)
- Müssen die Daten löschen, sobald sie nicht mehr benötigt werden
- Dürfen sie nicht kommerziell nutzen

Beispiel:

Bei Hochwasser kann eine Kommune Echtzeit-Sensordaten von Brücken anfordern, um Evakuierungen zu koordinieren.

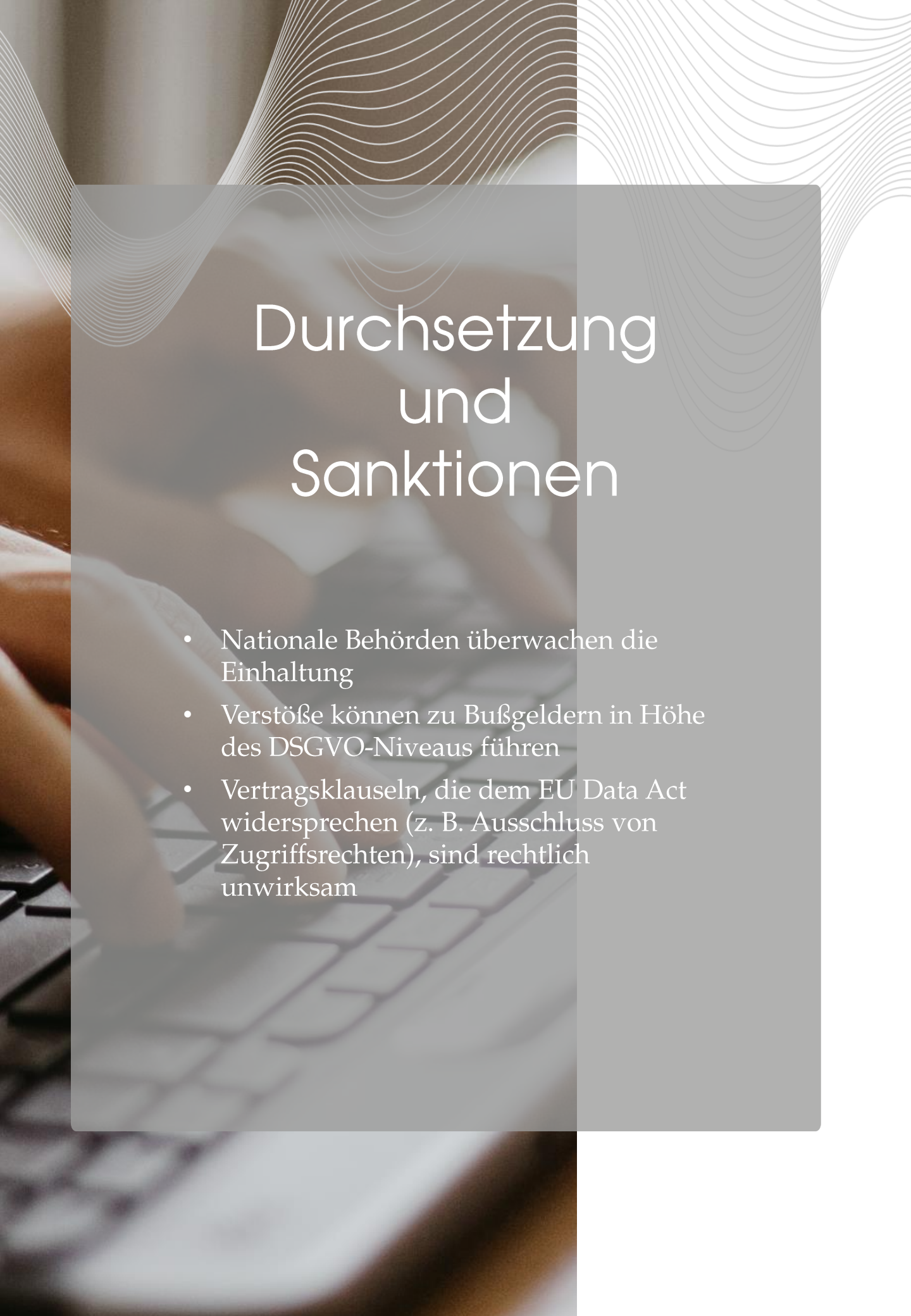
6

Statistische Ämter und Forschung

- Dürfen anonymisierte oder pseudonymisierte Daten für Zwecke im öffentlichen Interesse nutzen
- Müssen jede Re-Identifizierung verhindern
- Müssen den Umgang mit Daten transparent und sicher gestalten

Beispiel:

Ein Statistikamt nutzt Mobilitätsdaten zur Verkehrsplanung, ohne einzelne Fahrer identifizieren zu können.



Durchsetzung und Sanktionen

- Nationale Behörden überwachen die Einhaltung
- Verstöße können zu Bußgeldern in Höhe des DSGVO-Niveaus führen
- Vertragsklauseln, die dem EU Data Act widersprechen (z. B. Ausschluss von Zugriffsrechten), sind rechtlich unwirksam



Kurzfassung

Stakeholder	Zentrales Recht	Zentrale Pflicht
Nutzer	Zugriff & Weitergabe eigener Daten	Verantwortungsvolle Nutzung, klare Freigaben
Hersteller / Dateninhaber	Faire Kontrolle	Zugang, Transparenz & Sicherheit
Dritte	Datennutzung für klaren Zweck	Zweckgebundene Nutzung, Vertraulichkeit
Cloud-Anbieter	Sichere Datenverarbeitung	Wechsel ermöglichen, Lock-in vermeiden
Öffentliche Stellen	Zugriff im Notfall	Verhältnismäßigkeit & Datenschutz



Unser Team



Alexandra Popa
Chief Data Officer



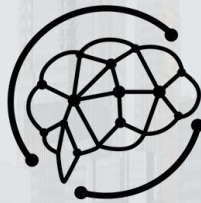
Paulina Marinos
Chief Operating Officer

VIELEN DANK

Fragen?
Kontaktieren Sie uns.



info@clarity-layer.com



CLARITY LAYER
DATA STRATEGY & GOVERNANCE