

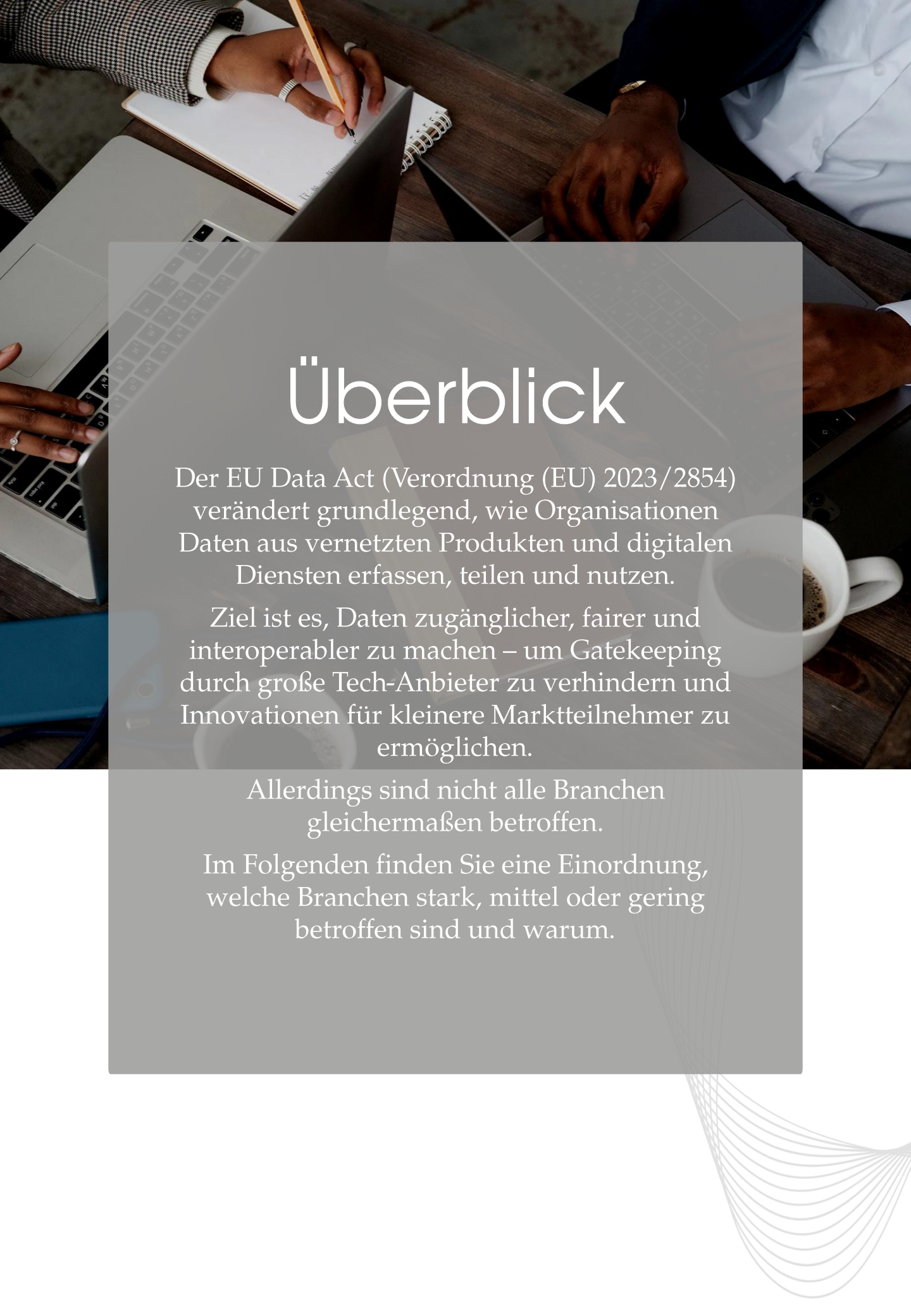
CLARITY LAYER
DATA STRATEGY & GOVERNANCE

Der EU Data Act Wer am stärksten betroffen ist

www.clarity-layer.com

Inhalt

- 01 Überblick
- 02 Stark betroffene Branchen
- 03 Mäßig betroffene Branchen
- 04 Gering betroffene Branchen
- 05 Zusammenfassung
- 06 Was Unternehmen tun sollten
- 07 Clarity Layer Einordnung



Überblick

Der EU Data Act (Verordnung (EU) 2023/2854) verändert grundlegend, wie Organisationen Daten aus vernetzten Produkten und digitalen Diensten erfassen, teilen und nutzen.

Ziel ist es, Daten zugänglicher, fairer und interoperabler zu machen – um Gatekeeping durch große Tech-Anbieter zu verhindern und Innovationen für kleinere Marktteilnehmer zu ermöglichen.

Allerdings sind nicht alle Branchen gleichermaßen betroffen.

Im Folgenden finden Sie eine Einordnung, welche Branchen stark, mittel oder gering betroffen sind und warum.



Stark betroffene Branchen

Diese Branchen erzeugen oder nutzen in hohem Maße Daten aus vernetzten Produkten, IoT-Geräten oder Plattformen. Der Data Act verändert unmittelbar, wie diese Daten verarbeitet, geteilt und monetarisiert werden.

Branche	Warum stark betroffen	Beispiele & Auswirkungen
Automobil & Mobilität	Fahrzeuge erzeugen enorme Mengen an Telemetrie- und Sensordaten (Standort, Leistung, Nutzungsverhalten). Der Data Act verpflichtet Hersteller, Nutzern und Dritten (z. B. Werkstätten) Zugang zu diesen Daten zu gewähren.	Autohersteller müssen Echtzeitdaten öffnen. Unabhängige Werkstätten, Versicherungen und Mobility-Startups können Zugriff anfordern. Geschäftsgeheimnisse bleiben geschützt – aber „Die Daten gehören uns“ reicht nicht mehr aus..
Fertigung & Industrial IoT	Industriemaschinen, Roboter und Produktionslinien erzeugen kontinuierlich Betriebsdaten. Der Data Act zwingt Hersteller, diese Daten fair mit Kunden und Partnern zu teilen.	Maschinenhersteller müssen Fabrikbetreibern Zugriff auf Leistungsdaten ermöglichen, anstatt sie hinter proprietären Dashboards zu verstecken
Smart Home & Consumer Electronics	Smarte Haushaltsgeräte, Wearables und Automationssysteme erfassen Nutzungs- und Personendaten. Der Data Act verlangt Transparenz, Interoperabilität und einfachen Nutzerzugang.	Smart-Home-Anbieter müssen den Export oder die Weitergabe von Gerätedaten an Drittanbieter ermöglichen. Abgeschlossene „Vendor-Lock-in“-Ökosysteme geraten unter Druck.
Landwirtschaft & AgriTech	Vernetzte Traktoren, Drohnen und Sensoren sammeln Umwelt- und Betriebsdaten. Landwirte erhalten explizite Rechte auf Zugang und Weitergabe dieser Daten.	Hersteller und Plattformen müssen Landwirten vollständigen Zugriff auf Boden-, Ertrags- und Maschinendaten gewähren. Drittanbieter können darauf aufbauend neue Services entwickeln.
Gesundheitswesen & MedTech	Medizinische Geräte erzeugen sensible Daten. Der Data Act ergänzt die DSGVO und stärkt Datenzugriffsrechte von Patienten und Einrichtungen.	Hersteller müssen relevante nicht-personenbezogene oder pseudonymisierte Daten unter fairen Bedingungen an Gesundheitsdienstleister oder Forschungseinrichtungen weitergeben.
Cloud- & Edge-Service-Anbieter	Der Data Act schafft starke Regeln zur Datenübertragbarkeit und zum Anbieterwechsel.	Cloud-Anbieter müssen Migrationshürden abbauen, Übertragungskosten transparent machen und unfaire Vertragsbindungen verhindern..

Mäßig betroffene Branchen

Diese Branchen sind datengetrieben, aber nicht primär auf vernetzte Produkte aufgebaut. Sie müssen Governance, Verträge und technische Strukturen anpassen.

Branche	Warum mäßig betroffen	Beispiele & Auswirkungen
Energie & Versorger	Smart Grids, Zähler und Infrastrukturen erzeugen Verbrauchs- und Nutzerdaten, die nun mit Kunden oder Behörden geteilt werden müssen.	Energieunternehmen müssen standardisierte APIs für Kundendaten bereitstellen und in Notfällen kooperieren.
Telekommunikation	Telekommunikationsunternehmen verarbeiten Netzwerk- und Gerätedaten und agieren häufig als Vermittler. Regelungen zu Datenteilung und Anbieterwechsel wirken sich auf die Interoperabilität von Diensten aus.	Telekommunikationsanbieter müssen die Portabilität von Nutzerdaten sicherstellen und transparent machen, wie Netzwerkdaten verwendet werden.
Logistik & Transport	Flotten- und Trackingsysteme erfassen große Mengen an Betriebsdaten. Nutzer und Partner erhalten neue Rechte, diese Daten anzufordern.	Flottenbetreiber können von Herstellern Fahrzeugleistungs- oder Sensordaten anfordern, um Routen zu optimieren.
Finanzdienstleistungen (insb. InsurTech)	Während Finanzdaten überwiegend durch PSD2 und DSGVO geregelt sind, fallen Versicherungen mit Telematik- oder IoT-Nutzung (z. B. Kfz-Versicherungen) unter den Data Act.	Versicherer können auf von Kunden autorisierte Daten aus Fahrzeugen oder Geräten zugreifen, müssen diese jedoch strikt zweckgebunden verarbeiten.
Forschung & Wissenschaft	Erhalten neue Möglichkeiten, nicht-personenbezogene Daten von privaten Unternehmen für Forschung im öffentlichen Interesse zu nutzen – auf Basis strukturierter Vereinbarungen.	Universitäten können anonymisierte IoT- oder Industriedaten anfordern, um Umwelt- oder gesellschaftliche Entwicklungen zu analysieren.
Öffentlicher Sektor & Statistikämter	Dürfen Daten aus dem Privatsektor ausschließlich in Notfällen oder bei klar definierten öffentlichen Bedürfnissen anfordern – unter verhältnismäßigen und sicheren Bedingungen.	Bei Überschwemmungen oder Pandemien können Behörden anonymisierte Sensor- oder Mobilitätsdaten von privaten Unternehmen anfordern.

Gering betroffene Branchen

Diese Branchen nutzen nur in begrenztem Umfang Daten aus vernetzten Geräten. Ihre Pflichten aus dem Data Act sind gering, auch wenn indirekte Effekte über Anbieter auftreten können.

Branche	Warum gering betroffen	Beispiele & Auswirkungen
Professionelle Dienstleistungen	Rechtsanwaltskanzleien, Beratungen und HR-Agenturen verarbeiten selten IoT- oder Daten aus vernetzten Produkten.	Sie müssen vor allem Datenportabilität und faire Verträge bei der Nutzung von SaaS- oder Cloud-Anbietern sicherstellen, sind ansonsten jedoch nur gering betroffen.
Einzelhandel (nicht smart)	Der klassische Einzelhandel nutzt Konsumentenanalysen (unter DSGVO), setzt jedoch nur wenige vernetzte Geräte ein.	Betroffen sind Unternehmen nur dann, wenn sie vernetzte Produkte verkaufen oder verwalten (z. B. smarte Haushaltsgeräte).
Bildung	Verarbeitet überwiegend personenbezogene Daten, weshalb die DSGVO stärker greift als der Data Act.	Relevant wird der Data Act nur bei der Nutzung vernetzter Lernsysteme oder KI-gestützter Bildungstools.
Immobilien & Bau	Einige neue Smart-Building-Technologien können begrenzte Verpflichtungen mit sich bringen.	Gebäudeeigentümer, die vernetzte Systeme nutzen, können Zugriffsrechte auf Leistungsdaten von Lieferanten erhalten.



Zusammenfassung

Betroffenheit	Branchen	Zusammenhänge
 Stark	Automobil, Industrial IoT, Smart Devices, Landwirtschaft, MedTech, Cloud	Hoher Einsatz vernetzter Produkte, Risiko von Daten-Lock-in, starke Regeln zu Datenteilung und Interoperabilität.
 Mäßig	Energie, Telekommunikation, Logistik, Finanzen (IoT), Forschung, öffentlicher Sektor	Mischung aus Nutzer- und Betriebsdaten, neue Pflichten zur Datenteilung und API-Bereitschaft.
 Gering	Dienstleistungen, Einzelhandel, Bildung, Immobilien	Vorwiegend indirekte Effekte durch Anbieter-Compliance oder Nutzung smarter Produkte.



Was Unternehmen tun sollten

1. **Datenflüsse erfassen** – Identifizieren Sie, welche Daten Ihre Produkte oder Systeme erzeugen und wer sie aktuell kontrolliert.
2. **Rolle einordnen** – Klären Sie, ob Sie Dateninhaber, Nutzer oder Datenempfänger im Sinne des Data Acts sind.
3. **Verträge prüfen** – Stellen Sie sicher, dass Regelungen zu Datenteilung, Portabilität und Compliance fair und zulässig sind.
4. **APIs oder Zugriffsmechanismen vorbereiten** – Insbesondere, wenn Sie vernetzte Produkte herstellen oder zugehörige Dienste anbieten.
5. **Teams schulen** – Technik, Recht und Vertrieb müssen die neuen Nutzerrechte verstehen.

Clarity Layer Einordnung

Der Data Act markiert das Ende des Hortens von Daten als Geschäftsmodell. Von Automobilherstellern bis zu Cloud-Anbietern müssen Unternehmen den Wandel vollziehen – weg vom Datenbesitz, hin zur verantwortungsvollen Ermöglichung von Zugriff.

Bei Clarity Layer unterstützen wir Organisationen dabei, diesen Wandel zu gestalten – mit Strukturen, ethischer Orientierung und Governance-Systemen, die Compliance in Vertrauen und Wettbewerbsvorteile übersetzen.

Unser Team



Alexandra Popa
Chief Data Officer



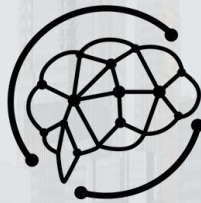
Paulina Marinos
Chief Operating Officer

VIELEN DANK

Fragen?
Kontaktieren Sie uns.



info@clarity-layer.com



CLARITY LAYER
DATA STRATEGY & GOVERNANCE