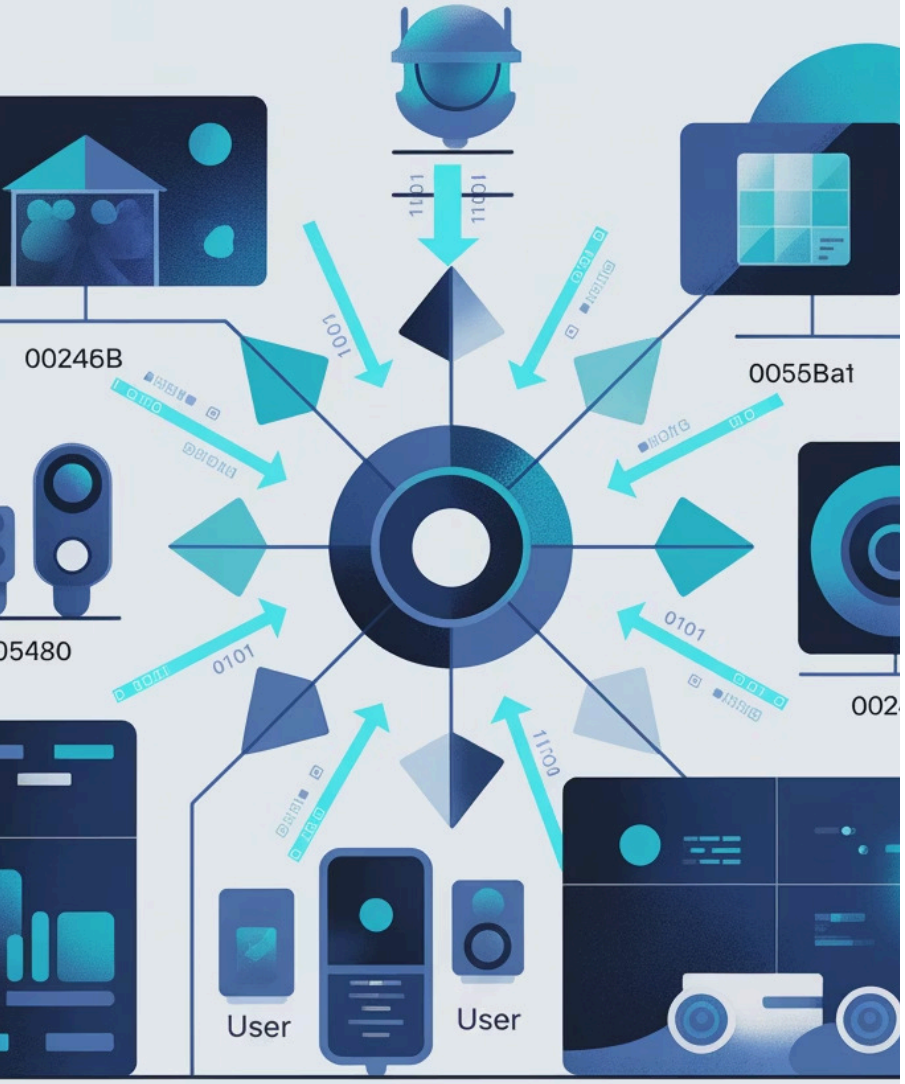


EU Data Act: Praxisleitfaden Teil 4

Praxistipps zu Datenzugangspflichten

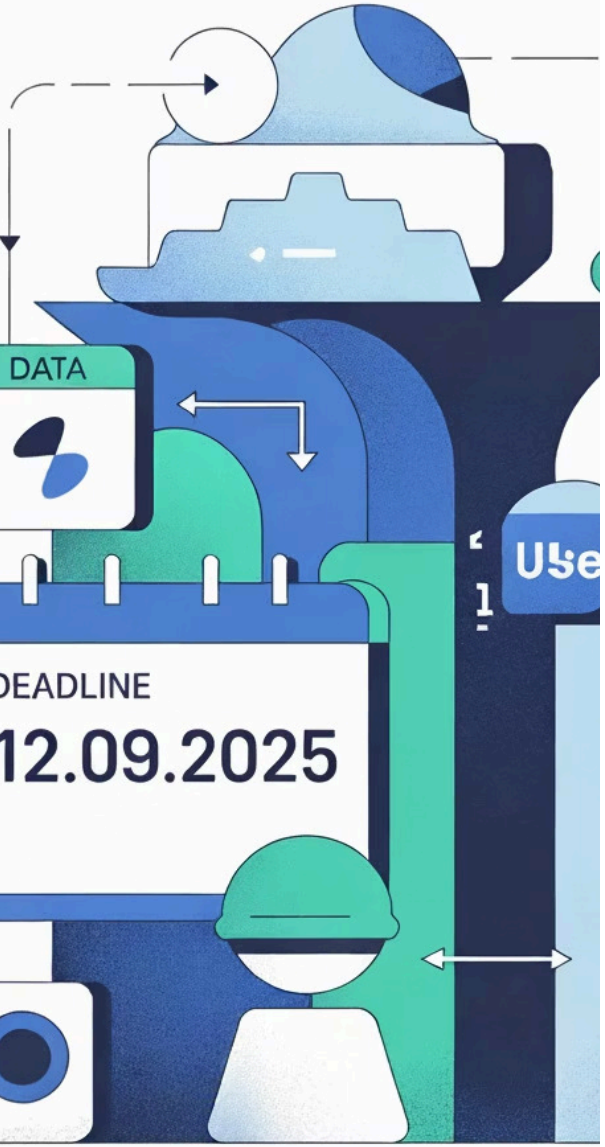
Der Data Act schafft umfassende Verpflichtungen und Herausforderungen für Anbieter vernetzter Produkte und verbundener Dienste.

Er regelt den Datenzugang für Nutzer, Informationspflichten und die Herausgabe und Nutzungsmöglichkeit von Daten durch Dritte.

Dieser fünfteilige Leitfaden zeigt konkret, was jetzt zu tun ist:

Er erklärt die wichtigen Regelungen, ihre praktischen Auswirkungen und gibt praxisnahe Tipps für Hersteller, Anbieter, Nutzer und Datenempfänger.

Business sichern, Risiken minimieren, Chancen nutzen.



Datenzugangspflichten: Der Überblick

Kernaspekte der neuen Regelungen:

- **Umfassender Geltungsbereich:** Betrifft viele IoT-Produkte und verbundene Diensten.
- **Betroffene Akteure:** Regelungen wirken sich auf Hersteller, Anbieter, Dateninhaber, Nutzer und Dritte aus.
- **Datenzugangsrechte für Nutzer:** Nutzer erhalten das Recht auf Zugang und Weitergabe der von ihren vernetzten Geräten generierten Daten an Dritte (z.B. Konkurrenten)
- **Informationspflichten für Anbieter:** Hersteller und Dateninhaber müssen transparent über Art, Zweck und potenzielle Weitergabe gesammelter Daten informieren.

⊗ Seit 12.09.2025 dürfen Dateninhaber Produktdaten und verbundene Dienstdaten nur mit vertraglicher Zustimmung des Nutzers für eigene Zwecke nutzen.

⚠ Produktbezogene Access-by-Design-Regelungen greifen bereits ab 12.09.2026.

Datenzugang - Varianten

Der Data Act verpflichtet zu drei Varianten des Datenzugangs, die unterschiedliche Anforderungen und Verpflichtungen mit sich bringen.

1. Direkte Zugänglichkeit durch Design (Art. 3)

Nutzer müssen standardmäßig direkten Zugang zu Daten auf vernetzten Geräten oder verbundenen Diensten haben

Erfasste Daten:

- Produktdaten
- Verbundene Dienstdaten

2. Zugang für Nutzer auf Anfrage (Art. 4)

Dateninhaber muss Daten auf Anfrage des Nutzers zur Verfügung stellen

Erfasste Daten:

- „Ohne Weiteres verfügbare“ Produktdaten
- „Ohne Weiteres verfügbare“ verbundene Dienstdaten

3. Zugang für Dritte auf Anfrage des Nutzers (Art. 5, 6)

Dateninhaber muss Daten auf Anfrage des Nutzers an Dritte (Datenempfänger) zur Verfügung stellen

Erfasste Daten:

- „Ohne Weiteres verfügbare“ Produktdaten

Access-by-Design (Art. 3)

Ab dem 12. September 2026 müssen alle vernetzten Produkte und verbundenen Dienste so gestaltet sein, dass Nutzer standardmäßig direkten und unkomplizierten Zugang zu bestimmten Daten haben.

Verpflichtete

Jeder in der Vertriebskette: Hersteller, Verkäufer, Wiederverkäufer, Vermieter von vernetzten Produkten oder verbundenen Diensten

Erfasste Daten

Produktdaten, verbundene Dienstdaten sowie relevante Metadaten und Erklärungen

Anforderungen Datenzugang

Einfacher, sicherer, kostenloser, kontinuierlicher Echtzeitzugriff auf Produktdaten und verbundene Dienstdaten in einem strukturierten, gängigen, maschinenlesbaren Format.

Praxistipp: Proaktive technische Gestaltung, die den Datenzugang von Anfang an ermöglicht und nicht als nachträgliche Funktion implementiert.

Anforderungen an den Datenzugang

Technische Anforderungen

- Standardmäßig verfügbar (keine Anfrage nötig)
- Direkt, soweit technisch durchführbar
- Einfach zugänglich (Self-Service)
- Sicher und kostenlos
- Umfassend: Alle relevanten Produktdaten, inkl. Betriebs-, Nutzungs- und Leistungsdaten
- Strukturiert in gängigen maschinenlesbaren Formaten (z.B. JSON, XML, CSV)

Umsetzungsmöglichkeiten

- Kabel-/Drahtlosschnittstelle direkt am Gerät
- Server oder Self-Service-Portal im Internet (für verbundene Dienste)
- API mit vollständiger Dokumentation
- Authentifizierungs- und Autorisierungsmechanismen nötig

Praxistipp: Verschlüsselte Daten müssen entschlüsselt und proprietäre Formate angepasst werden. Der Nutzer benötigt die Entschlüsselungsschlüssel.

Geschäftsgeheimnisse bei Access-by-Design

Beim Access-by-Design gibt es keinen direkten Schutz für Geschäftsgeheimnisse. Da Nutzer auch Konkurrenten sein können, müssen Dateninhaber alternative Strategien entwickeln, um Geschäftsgeheimnisse nicht verfügbar machen zu müssen.

1

Datenverzicht

Auf bestimmte sensible Daten verzichten

2

Datenveredelung

Daten im Gerät mit nachweisbaren Investitionen veredeln

3

Vertragliche Regelung

Separate Vereinbarungen (rechtlich unsicher)

Datenzugang für Nutzer und Datenemfänger (Art. 4-6)

Der Dateninhaber muss auf Anfrage des Nutzers bestimmte Daten an verschiedene Empfänger herausgeben.

Die Anforderungen unterscheiden sich je nach Empfängertyp.

Dateninhaber

Verantwortlich für die Herausgabe von Daten

Alternative 1: Nutzer (Art. 4)

Herausgabe 'ohne Weiteres verfügbarer'

Produkt- und verbundener Dienstdaten auf Anfrage des Nutzers

Alternative 2: Dritte (Atenempfänger) (Art. 5, 6)

Herausgabe 'ohne Weiteres verfügbarer'

Produkt- und verbundener Dienstdaten auf Anfrage des Nutzers an Dritte

Datenzugang Nutzer (Art. 4)

Dateninhaber müssen alle "ohne Weiteres verfügbaren" Produktdaten und verbundenen Dienstdaten herausgeben, die der Nutzer nicht bereits selbst abrufen kann.

01

Unverzüglich und einfach

Unkomplizierte Bereitstellung ohne Verzögerung über technische Schnittstellen (APIs) oder Datenportale

02

Sicher und kostenlos

Geschützter Zugang; Nutzeridentifizierung nur soweit für Bereitstellung erforderlich, Gewährleistung Datenschutz

Ohne Gebühren für Nutzer

03

Umfassend und strukturiert

Alle relevanten Daten in gängigem, maschinenlesbarem Format

04

Gleiche Qualität wie für Dateninhaber

05

Kontinuierlich und in Echtzeit

Soweit technisch möglich

Was sind "Ohne Weiteres verfügbare Daten"?

Der Dateninhaber muss nur **"ohne Weiteres verfügbare Daten"** herausgeben: Dies sind Daten, die das Produkt oder der Dienst im normalen Betrieb generiert, ohne dass der Anbieter eine wesentliche zusätzliche Verarbeitung oder Ableitung vornehmen muss.

✅ Was zählt dazu?

- **Direkt generierte Betriebsdaten:** Daten, die unmittelbar durch die Funktion des Produkts entstehen (z.B. Temperatur eines Smart-Thermostats, Laufzeiten einer Waschmaschine).
- **Leistungs- und Nutzungsdaten:** Informationen über Effizienz oder Gebrauch des Produkts (z.B. Energieverbrauch, Nutzungshäufigkeit bestimmter Funktionen, Fehlermeldungen).
- **Sensorwerte:** Rohdaten von integrierten Sensoren (z.B. GPS-Position eines Fahrzeugs, Feuchtigkeitswerte eines intelligenten Bewässerungssystems).
- **Maschinenlesbare Formate:** Daten, die in gängigen, strukturierten und maschinenlesbaren Formaten (wie JSON, XML, CSV) ohne proprietäre Hürden vorliegen.

❌ Was zählt nicht dazu?

- **Abgeleitete oder "veredelte" Daten:** Informationen, die erst durch komplexe Algorithmen oder proprietäre Analysen des Herstellers gewonnen werden (z.B. voraussichtliche Lebensdauer basierend auf Nutzungsdaten).
- **Geschäftsgeheimnisse:** Daten, die keinen direkten Bezug zur Leistung oder Nutzung des Produkts durch den Kunden haben, sondern dem Kern-IP des Anbieters zuzuordnen sind.
- **Hochgradig personalisierte Daten:** Inhalte, die der Anbieter basierend auf Nutzerprofilen generiert, und deren Weitergabe die Privatsphäre anderer Nutzer beeinträchtigen könnte.
- **Verschlüsselte Daten ohne Entschlüsselungsmechanismus:** Wenn Anbieter selbst keinen direkten Zugang zu entschlüsselten Rohdaten hat oder dieser Zugang eine Sicherheitsverletzung wäre.

Praxistipp: Rohdaten direkt im Gerät durch nachweisbare erhebliche Investitionen oder Know-How veredeln und aufbereiten um Herausgabe zu verhindern.

"Ohne Weiteres verfügbare Daten" - Problemfälle

Datenschutz

Auch "ohne Weiteres verfügbare" Daten können personenbezogen sein. Die Anforderungen der DSGVO sind zu beachten die eine Herausgabe vielleicht nicht erlauben.

Komplexität der Nutzung

Die Bereitstellung der Rohdaten entbindet den Dateninhaber nicht von der Pflicht, verständliche Informationen bereitzustellen, auch wenn die Interpretation der Daten durch Dritte erfolgt.

Produktentwicklung vs. Nutzerwert

Eine klare Abgrenzung muss getroffen werden, welche Daten primär dem Nutzerwert dienen und welche ausschließlich für interne Entwicklungszwecke des Herstellers relevant sind.

Software-Updates

Änderungen in der Software des Produkts dürfen den Datenzugang nicht unrechtmäßig einschränken oder die Datenqualität mindern.

Die Identifikation von "ohne Weiteres verfügbaren Daten" erfordert eine genaue technische und rechtliche Bewertung der Datenströme in vernetzten Produkten und verbundenen Diensten.

Einschränkungen von "Ohne Weiteres verfügbar"

Keine Verfügbarkeit der Daten

und

Keine Pflicht

- zur erneuten Programmierung
- zu unverhältnismäßigem Aufwand zur Beschaffung

Aber erforderlich

- Zuordnung der Daten zu Nutzer / Produkt / Dienst muss möglich sein
- Kontinuierliche Bereitstellung

Technische Grenzen

- Echtzeit nur falls technisch durchführbar

Vorvertragliche Informationspflichten

Vor Vertragsschluss müssen dem Nutzer umfassende Informationen über Datenzugang und -nutzung bereitgestellt werden. Die Anforderungen unterscheiden sich für vernetzte Produkte und verbundene Dienste.

Vernetzte Produkte (Art. 3(2))

Verpflichtet: Jeder in der Vertriebskette

Inhalt: Informationen über abrufbare Daten und Zugangsmöglichkeiten

Zeitpunkt: Vor Vertragsschluss

Verbundene Dienste (Art. 3(3))

Ausführlichere Informationen über:

- Identität des Anbieters (Dateninhaber)
- Generierte/gesammelte Daten
- Zugriffsmöglichkeiten für Nutzer
- Weitergabe an Dritte (nur innerhalb EU)

Praxistipp: Bei mehreren Nutzern (z.B. Leasinggeber und -nehmer) muss jeder einzeln informiert werden!

Schutz von Geschäftsgeheimnissen

Bei der Herausgabe können Geschäftsgeheimnisse durch verschiedene Maßnahmen geschützt werden.

Schutzmaßnahmen

NDA, Nutzungsbeschränkungen, technische Maßnahmen. Geschäftsgeheimnis muss deklariert werden.

Verweigerung Herausgabe von Geschäftsgeheimnissen

Bei hoher Wahrscheinlichkeit schweren wirtschaftlichen Schadens: Verweigerung möglich, aber Behörde muss informiert werden.

Nutzungsverbote

Keine Nutzung zu Wettbewerbszwecken

Keine Entwicklung konkurrierender Produkte

Kein Einsatz von Zwangsmitteln um an Daten zu kommen

Weitere Einschränkungen der Herausgabepflicht

Personenbezogene Daten

Nutzer muss Rechtsgrundlage nach DSGVO nachweisen. Dateninhaber kann bei Unklarheit anonymisieren und trägt Verantwortung für rechtmäßige Herausgabe.

Ausnahme: Nutzer = betroffene Person (Art. 15, 20 DSGVO).

Sicherheitsgründe

Einschränkung Herausgabe möglich, wenn Sicherheitsanforderungen (NIS2, BSIG, Cyber Resilience Act) beeinträchtigt werden oder Risiken für Gesundheit, Sicherheit oder Schutz entstehen.

Historische Daten

Neuer Nutzer hat grundsätzlich Anspruch auf alle vorhandenen Produktdaten, auch aus der Zeit vor seiner Nutzung.

Einschränkung durch Datenschutzrechte früherer Nutzer.

Datenzugang für Nutzer (Art. 4)

Der Nutzer hat Anspruch auf Herausgabe von Daten durch den Dateninhaber. Es gibt jedoch wichtige Bedingungen, Ausnahmen und Ablehnungsgründe.

Nutzungsrechte (Nr. 1-3)

- Freie Nutzung für jeden Zweck
- Weitergabe an Dritte
- Daten durch Dateninhaber nicht privilegiert verwendbar (Erwägungsgrund 30)

Mögliche Beschränkungen / Ablehnungsgründe

- Ablehnung Herausgabe oder Beschränkung des Datenumfangs, wenn Geschäftsgeheimnisse enthalten; oder Sicherheitsanforderungen oder Schutz von Gesundheit / Sicherheit beeinträchtigt
- **Verweigerung des Zugangs wenn schwere wirtschaftliche Schäden erwartbar**
- Verbot zur Entwicklung konkurrierender vernetzter Produkte

Durchsetzung des Zugangs (Nr. 10)

- Verweigerung / Einschränkung des Datenzugang nur mit Information der zuständigen Behörde; mit nachfolgendem Verfahren zur Durchsetzung des Zugangs auf Antrag des Datenempfängers

Herausgabe an Dritte - Datenempfänger (Art. 5)

Auf Wunsch des Nutzers müssen Dateninhaber "ohne weiteres Verfügbare" Daten auch Dritten zugänglich machen. Dies ermöglicht beispielsweise konkurrierenden Wartungsanbietern den Zugang zu Produktdaten.

Entgelt möglich

Vom Dritten kann Entgelt verlangt werden: Selbstkosten + Investitionsbeitrag + Marge (außer bei KMU/Non-Profit)

FRAND-Vergütung

Fair, angemessen und nicht-diskriminierende Vergütung für Datenzugang (nicht für KMU)

Vertragspflicht

Vereinbarung mit Datenempfänger zu Nutzungsrechten & Nutzungsbeschränkung erforderlich (Art. 8-13)

Herausgabeverbot an

- Dritte außerhalb der EU
- "Torwächter" nach Digital Markets Act (Google, Meta, Microsoft etc.)

Risiken: Datenübermittlung an Wettbewerber

Die Pflicht zur Datenbereitstellung an Dritte – einschließlich direkter Wettbewerber – führt zu den größten Risiken für Dateninhaber.

Wettbewerbsrisiko

Konkurrenten erhalten Zugang zu wertvollen Betriebs-, Nutzungs- und technischen Daten, die trotz Schutzklauseln missbräuchlich genutzt werden könnten.

Geschäftsgeheimnisse

Müssen grundsätzlich offengelegt werden. Die nachträgliche Rechtsdurchsetzung ist komplex, während der Schaden bereits eingetreten sein kann.

FRAND-Vergütung = Monetarisierungshindernis

Dateninhaber dürfen nur FRAND (Fair, Reasonable and Non-Discriminatory) - konforme Vergütung verlangen – oft nur kostendeckend. Bei KMU-Empfängern nur Kosten für Erhebung und Bereitstellung. Eine Monetarisierung des Datenwertes ist damit eingeschränkt.

Kartellverbot (Art. 101 AEUV)

Informationsaustausch zwischen Wettbewerbern kann kartellrechtswidrig sein. Bei Verstößen drohen Milliardenbußgelder, Schadensersatz, Ausschluss von Aufträgen und strafrechtliche Sanktionen.

Praxistipp: Dateninhaber müssen proaktiv die folgenden Ausnahmen und Schutzmöglichkeiten nutzen, um die Datenherausgabe zu vermeiden oder soweit wie möglich einzuschränken.

Datenzugang für Datenempfänger (Art. 5)

Der Dateninhaber muss nur "ohne Weiteres verfügbare Daten" herausgeben:

Herauszugebende Daten: "ohne Weiteres verfügbare" Daten (Rohdaten)

- Direkt generierte Betriebsdaten
- Leistungs- und Nutzungsdaten
- Sensorwerte

Nicht herauszugebende Daten

- Veredelte Daten: Aus Rohdaten gefolgerte oder abgeleitete Informationen, die Ergebnis zusätzlicher erheblicher Investitionen des Herstellers (z.B. komplexe proprietäre Algorithmen oder Analysen)
- Daten sind für Datenempfänger bereits verfügbar und einfache Weitergabe nicht möglich
- Anderweitig gesammelte Daten die nur zur Speicherung oder weiteren Übermittlung an Gerät übermittelt wurden und von dort wieder abgerufen werden können
- Personenbezogene Daten sofern keine Rechtsgrundlage für Weitergabe

Praxistipp: Rohdaten direkt im Gerät durch nachweisbare erhebliche Investitionen oder Know-How veredeln und aufbereiten um Herausgabe zu verhindern.

Ablehnung der Datenherausgabe (Art. 5-10)

Dateninhaber können die Bereitstellung von Daten an Dritte (insbesondere Wettbewerber) unter engen Voraussetzungen verweigern oder einschränken:

1. Schutz von Testdaten (Art. 5 Abs. 2)

- **Gegenstand:** Daten aus der Erprobung neuer Produkte, Stoffe oder Verfahren, die noch nicht am Markt verfügbar sind.
- **Einschränkung:** Herausgabe kann verweigert werden, sofern keine anderweitige vertragliche Vereinbarung besteht.
- **Praxis-Risiko:** Kommerzielle Beta-Tests können ungewollt Datenzugriff für Wettbewerber eröffnen (''Early-Access-Dilemma'')

2. Nicht-Erforderlichkeit von Geschäftsgeheimnissen (Art. 5 Abs. 9-11)

- **Offenlegungsgrenze:** Geschäftsgeheimnisse müssen gegenüber Dritten nur offengelegt werden, wenn dies für den vereinbarten Zweck zwischen Nutzer und Drittempfänger **unbedingt erforderlich** ist.
- **Praxistipp:** Dateninhaber sollte vom Nutzer die Offenlegung des vereinbarten Zwecks zu verlangen, um die Erforderlichkeit der Datenherausgabe prüfen zu können.

3. Schutz von Geschäftsgeheimnissen (Art. 5 Abs. 11 & 12)

- **Voraussetzung:** Nachweis, dass trotz Schutzmaßnahmen ein **schwerwiegender wirtschaftlicher Schaden** durch die Offenlegung droht.
- **Verfahren:** Die Ablehnung muss schriftlich begründet und gegenüber dem Nutzer/Empfänger detailliert dargelegt werden.
- **Behördenkontrolle:** Zuständige Behörde kann Verweigerung auf Antrag prüfen und ggf. Herausgabe unter spezifischen Schutzauflagen anordnen.

Nutzungsrechte & Nutzungsbeschränkungen (Art. 6, 8, 9)

Klare Nutzungsregeln und -beschränkungen sind essenziell, um trotz gesetzlicher Herausgabepflichten die Kontrolle über wettbewerbsrelevante Daten zu behalten und den Missbrauch von Know-how durch Dritte zu verhindern.

Nutzungsrechte des Datenempfängers

- **Zweckbindung:** Nutzung der Daten nur für mit Nutzer vertraglich vereinbarten Zweck
- **Art. 8 (FRAND-Prinzip):** Datenbereitstellung muss gegen faire, angemessene Vergütung und diskriminierungsfrei erfolgen (Ausnahme: wenn Empfänger KMU ist).
- Entgelt für Datenbereitstellung kann erhoben werden, muss aber Wettbewerb nicht behindern

Nutzungsbeschränkungen des Datenempfängers

- **Wettbewerbsverbot:** Keine Entwicklung konkurrierender Produkte oder verbundener Dienste
- **Weitergabeverbot:** Keine Weitergabe an andere Dritte ohne ausdrückliche Zustimmung des Nutzers,
- **Gatekeeperverbot:** Keine Weitergabe von Daten an Gatekeeper
- **Sicherheit:** Keine Nutzung, die die Sicherheit des Produkts oder Dienstes gefährden könnte.
- **Profiling-Verbot:** Keine Verwendung der Daten, um detaillierte Einblicke in die wirtschaftliche Lage oder Produktionsmethoden des Dateninhabers zu gewinnen.

Praxistipp: Zusätzlich zu den obligatorischen Klauseln sollten spezifische Nutzungsbedingungen geregelt werden. Datenherausgabe über neutrale Datenintermediäre prüfen.

Data Act vs. DSGVO: Fundamentale Widersprüche

Der Data Act gilt neben der DSGVO. Wenn die vom Data Act erfassten Daten personenbezogene Daten sind müssen beide Verordnungen eingehalten werden - auch wenn diese gegenteiliges fordern.

1

Keine eigenständige Rechtsgrundlage

Data Act ist keine eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Art. 6 DSGVO – es muss stets eine zusätzliche datenschutzrechtliche Rechtsgrundlage vorliegen.

2

Der fundamentale Widerspruch

Der Data Act verpflichtet den Dateninhaber zur Herausgabe von Daten, während die DSGVO die Verarbeitung und Weitergabe personenbezogener Daten in vielen Fällen verbietet.

3

Das Haftungsdilemma

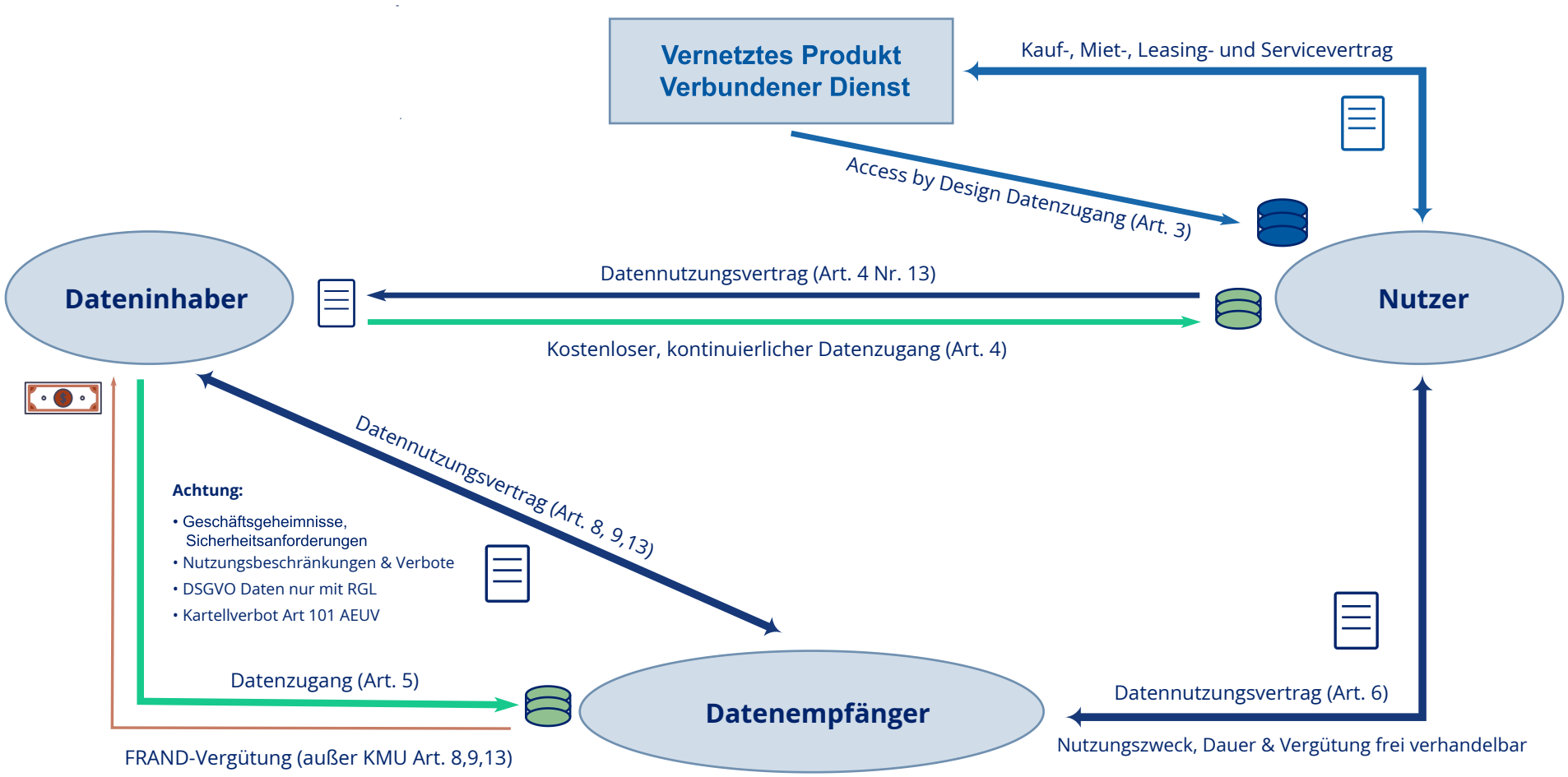
Wenn ein Dateninhaber (der nicht die betroffene Person ist) personenbezogene Daten Dritter (z.B. des Nutzers) an Datenempfänger weitergeben muss, entsteht ein Dilemma zwischen Herausgabepflicht nach Data Act und Verarbeitungsverbot nach DSGVO.

Kritisch: Unternehmen können gleichzeitig gegen beide Verordnungen verstoßen.

Praxistipp: Eine sorgfältige Datenklassifizierung, strikte Trennung personenbezogener und nicht-personenbezogener Daten und rechtskonforme Datenflüsse mit technischen und Organisatorischen Schutzmaßnahmen wie Pseudonymisierung und Anonymisierung sind zwingend erforderlich.

Rechtliche und kommerzielle Beziehungen

Der Data Act führt zu komplexen vertraglichen und kommerziellen Verhältnissen zwischen allen beteiligten Parteien.



Hauptverträge Hersteller-Nutzer

Kauf-, Miet-, Leasing- oder Serviceverträge zwischen Hersteller/Anbieter und jedem einzelnen Nutzer als Grundlage der Produktnutzung.

Datennutzungsverträge mit Nutzer (Art. 4 Nr. 13)

Zwingende spezifische Vereinbarungen zu Umfang und Bedingungen der Datennutzung durch Anbieter .

Zugangsbedingungen (Art. 4)

Technische und organisatorische Regelungen für kostenlosen, kontinuierlichen Echtzeit-Datenzugang des Nutzers.

Datennutzungsvertrag mit Datenempfängern (Art. 6)

Nutzungszweck und Dauer, Einschränkungen, Vertraulichkeit, Schutzmaßnahmen (TOM), Sanktionen, FRAND Vergütung

Prozess: Datenzugangsanfrage Teil 1

Für Nutzer (eigener Zugang) oder Datenempfänger (Drittzugang)

Antragseingang

- Nutzerantrag beim Dateninhaber auf Datenherausgabe an sich oder benannten Dritten
- Schriftliche/elektronische Autorisierung des Nutzers

Identitätsprüfung & Berechtigungsprüfung

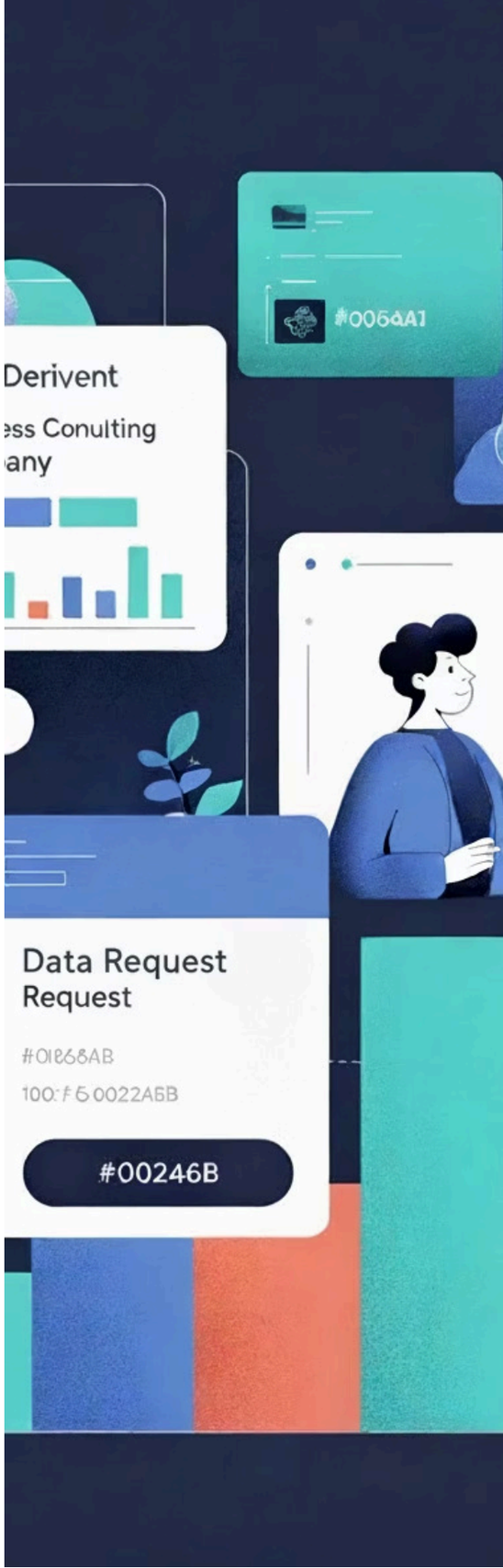
- Verifizierung der Berechtigung des Antragstellers
- Sicherstellung der Authentizität der Anfrage
- Prüfung, ob direkter Zugang nach Art. 3 möglich ist

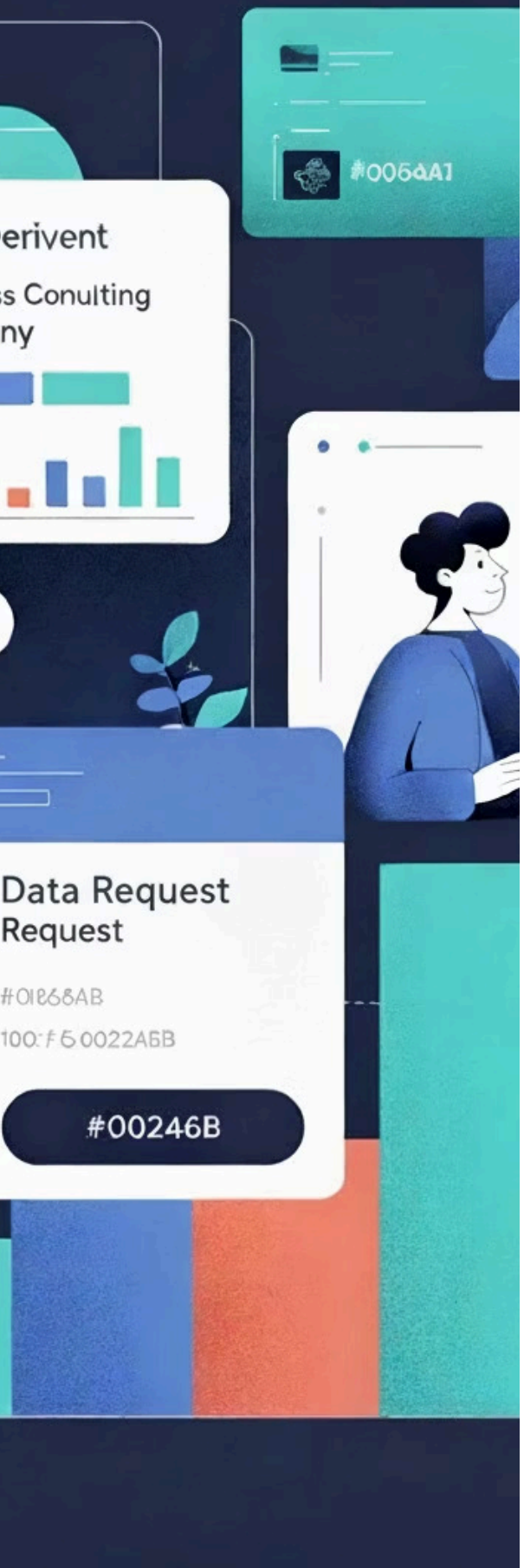
Datenklassifizierung

- Produktdaten oder verbundene Dienstdaten? → Umfang des Zugangsrechts prüfen
- "Ohne Weiteres verfügbare Daten"? → Herausgabepflicht
- Veredelte Daten ? → Ggf. ausgenommen von Herausgabepflicht

Datenklassifizierung (DSGVO-Compliance)

- **Kritisch:** Prüfung, ob personenbezogene Daten betroffen sind
- Trennung personenbezogener und nicht-personenbezogener Daten
- Rechtsgrundlage für Datenherausgabe nach Art. 6 DSGVO prüfen
- Ggf. Pseudonymisierung/Anonymisierung durchführen





Prozess: Datenzugangsanfrage Teil 2

Prüfung und vertragliche Absicherung

Prüfung von Ablehnungsgründen

- Empfänger = Gatekeeper? → Weitergabe verboten
- Empfänger = Wettbewerber? → Kartellverbot prüfen (Art. 101 AEUV)
- Testdaten betroffen? → ggf. keine Herausgabepflicht
- Geschäftsgeheimnisse betroffen und erforderlich? → Möglicher Ablehnungsgrund
- Sicherheitsanforderungen gefährdet? → Möglicher Ablehnungsgrund
- Weitere Ablehnungsgründe gegeben?

→ Bei Ablehnung: Begründete Ablehnung an Antragsteller mit Verweis auf gesetzliche Ausnahmen

→ Bei Genehmigung: Weiter zu Checkpoint 5

Vertragliche Absicherung bei Drittzugang

- Definition Nutzungszweck und -dauer
- Nutzungsbeschränkungen festlegen:
  - Zweckbindung
  - Wettbewerbsverbot (Definition der nicht verbotenen konkurrierenden Produkte)
  - Weitergabeverbot an Dritte
  - Sicherheitsanforderungen
- NDA/Vertraulichkeitsverpflichtung inkl. Vertragsstrafen
- Schutz von Geschäftsgeheimnissen (TOM)

Vergütung festlegen

- FRAND-konforme Vergütung vereinbaren
- Ausnahme: Bei KMU als Empfänger nur kostendeckend

Prozess: Datenzugangsanfrage - Teil 3

Bereitstellung und Compliance

Datenbereitstellung

- Unverzügliche Bereitstellung in strukturiertem, maschinenlesbarem Format
- Bei Vereinbarung: Kontinuierlicher Echtzeit-Zugang über definierten Zeitraum
- Alternative prüfen: Bereitstellung über neutrale Datenintermediäre

Compliance-Dokumentation

- Dokumentation aller Schritte für Nachweispflichten
- Monitoring der Datennutzung durch Empfänger
- Regelmäßige Überprüfung der Einhaltung vertraglicher Verpflichtungen

Zeitplan und Umsetzung

1 — **12.09.2025**

Nutzungsbeschränkung ist bereits in Kraft. Dateninhaber benötigen vertragliche Zustimmung zur Datennutzung für eigene Zwecke.

2 — **12.09.2026**

Access-by-Design wird verpflichtend. Alle neuen Produkte müssen konform sein.

3 — **Laufend**

Informationspflichten, Herausgabepflichten und Schutzmaßnahmen müssen umgesetzt werden.

Die Datenzugangspflichten erfordern umfassende technische und vertragliche Anpassungen.

⚠ Dateninhaber sollten dringend mit der Implementierung beginnen, um Compliance sicherzustellen und Produkte, Geschäftsmodelle und wertvolle Assets angemessen zu schützen.

Fortsetzung folgt: Ihr Weg durch die Data-Act-Transformation

Die kommenden Teile dieses Leitfaden beleuchten entscheidende Details und Praxistipps für die erfolgreiche Umsetzung des Data Act.

Teil 5: Wechsel von Datenverarbeitungsdiensten

Vertragliche, operative und kommerzielle Lösungen beim Anbieterwechsel

Bleiben Sie dran!

info@pri.com.de

www.pri-com.de

Von der Strategie bis zur Umsetzung
Wir begleiten Sie bei der Data-Act-Transformation:
Business sichern, Risiken minimieren, Chancen nutzen.

Data-Act-Beratung anfragen

Click here

Kostenloser Data-Act-Check

Ihre Betroffenheit in 5 Minuten prüfen

Click here

Mehr zum Data Act

Click here

Kostenloses Data Act Readiness Assessment & Checkliste herunterladen.

Click here