

BVMed RechtsKompass, 17. September 2026

EU Data Act – Überblick und Umsetzung für Medizinprodukteanbieter

Dr. Markus Fuderer
Rechtsanwalt

www.meisterernst.com
Fuderer@meisterernst.com

Agenda

- I Data Act aus Sicht der MedTech-Branche: Welche Unternehmen sind betroffen und in welchem Umfang?
- II Ist mein Medizinprodukt ein vernetztes Gerät oder ein verbundener Dienst im Sinne des Data Act?
- III Accessibility by Design: Anforderungen an die Konzeption des Produkts
- IV Recht auf Datenzugang und Pflicht zur Datenbereitstellung gegenüber Nutzern und Dritten; vertragliche Gestaltungsmöglichkeiten und Schutz von Geschäftsnissen
- V Anforderungen beim Wechsel zwischen Datenverarbeitungsdiensten
- VI Übergangsfristen für die Produktumstellung

Data Act aus Sicht der MedTech-Branche: Welche Unternehmen sind betroffen und in welchem Umfang?

Rechtsrahmen, EHDS-Abgrenzung, Adressatenkreis, KMU-Ausnahmen und Durchsetzung.

Regelungsgehalt und Adressaten EU Data Act

- **Zielsetzung:** Förderung datenbasierter Wertschöpfung und datengetriebener Innovation
- **Adressatenkreis:** Nutzer, Dateninhaber (insb. Hersteller/Anbieter vernetzter Produkte und verbundener Dienste) sowie Dritte als potentielle Datenempfänger
- Neue Regelungen für Zugang, Nutzung und Weitergabe von Daten aus vernetzten Produkten und verbundenen Diensten (vgl. insb. Kapitel II, III DA)
- **Nutzerrechte:** Nutzer erhalten Zugriff auf die generierten Daten und können über Weitergabe entscheiden
- **Pflichten der Dateninhaber:** Verpflichtung zur Datenbereitstellung an Nutzer (Art. 3, 4 DA) und auf deren Verlangen an Dritte (Art. 5 DA)
- **Datenbereitstellung:** Zugang muss transparent, fair, angemessen und nichtdiskriminierend (FRAND) erfolgen (vgl. Art. 8, 13 DA).

Adressatenkreis nach dem Data Act

Direkte Factsheet-Beispiele – visuell auf den MedTech-/Digital-Health-Kontext zugespitzt

Beispielbasis: Smartwatch als vernetztes Produkt, Hersteller/verbundene App sowie externer Analyse-, Reparatur- oder Wartungsdienst.

Nutzerin / Nutzer



Definition

Person oder Einrichtung, die ein vernetztes Produkt nutzt.

Beispiel

Smartwatch-Nutzerin bzw. -Nutzer.

Dateninhaber



Definition

Hersteller bzw. Anbieter des verbundenen Dienstes, die bzw. der über die Daten verfügt und sie bereitstellt.

Beispiel

Hersteller der Smartwatch bzw. Anbieter der verbundenen App.

Datenempfänger / Dritter



Definition

Dritter, der auf Verlangen der Nutzerin bzw. des Nutzers Daten erhält.

Beispiel

Externer Analyse-, Reparatur- oder Wartungsdienstleister.

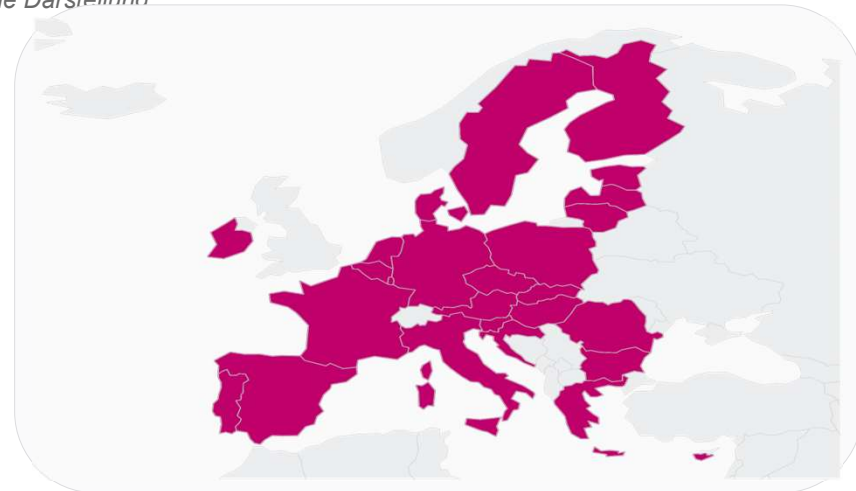
Räumlicher Anwendungsbereich des Data Act

EU-Marktbezug als Anknüpfungspunkt – anschaulich dargestellt mit einer echten EU-Karte

Kernaussagen

- Der Data Act folgt einem Markttortprinzip.
- Maßgeblich ist, ob ein vernetztes Produkt oder ein verbundener Dienst in der EU bereitgestellt oder genutzt wird.
- Ein Unternehmenssitz außerhalb der EU steht der Anwendbarkeit nicht entgegen.
- Auch ein Dateninhaber außerhalb der EU kann erfasst sein, wenn er Daten eines EU-Nutzers im Zusammenhang mit einem EU-Produkt bzw. -Dienst verarbeitet.

Schematische Darstellung



Dateninhaber
außerhalb der EU



Produkt / Dienst /
Nutzer in der EU

EU-Marktbezug → Data Act anwendbar

Anwendungsbereich EU Data Act

Ausnahmeregelungen für kleine- und mittlere Unternehmen

Größenklasse	Beschäftigte	Jahresumsatz/Bilanzsumme
Kleinstunternehmen	bis 9	und bis 2 Mio. Euro / 2 Mio. Euro
Kleine Unternehmen	bis 49	und bis 10 Mio. EUR / 10 Mio. Euro
Mittlere Unternehmen	bis 249	und bis 50 Mio. EUR / 43 Mio. Euro
Großunternehmen	über 249	oder über 50 Mio. EUR / 43 Mio. Euro

(Quelle: abgerufen am 2.02.2026 <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/DataAct/Hintergrund/1-Daten/start.html>)

- Die Ausnahme gilt jedoch nicht, wenn
 - das Kleinst- oder Kleinunternehmen ein „Partnerunternehmen“ hat oder Teil eines Konzernunternehmens ist, das selbst kein Kleinst- oder Kleinunternehmen ist, oder wenn
 - das Unternehmen als Unterauftragnehmer mit der Herstellung oder der Konzeption des vernetzten Produkts oder der Erbringung des
- Erleichterung: Die Pflichten des Kapitels II gelten für Daten aus Produkten bzw. verbundenen Diensten von Kleinst- und Kleinunternehmen grundsätzlich nicht; für bestimmte mittlere Unternehmen gilt die Ausnahme zeitlich begrenzt (Art. 7 Abs. 1 Data Act).

Deutsches Umsetzungsgesetz zum Data Act

DADG: Zuständigkeiten, Aufgabenteilung und Sanktionen

Meisterernst

Rechtsanwälte

Name: Datenverordnung-Anwendungs-und-Durchsetzungs-Gesetz (DADG) | **Ausfertigung:** 26.05.2026 | **Inkrafttreten:** 30.05.2026

1 | Zuständigkeit der Bundesnetzagentur

- Zentrale zuständige Behörde für Anwendung und Durchsetzung der Datenverordnung.
- Zentrale Anlaufstelle, allgemeine und besondere Beschwerden, nationale Aufsicht.
- Zuständig u. a. für Streitbeilegungsstellen, Datenverlangen öffentlicher Stellen und Handlungsempfehlungen.
- Durchsetzung: Ermittlungen, Auskunftsverlangen, Abhilfeverlangen und Anordnungen; Zwangsgeld bis 500.000 EUR.

2 | Abgrenzung zur Datenschutzaufsicht

- BfDI ist für nicht-öffentliche Stellen zuständige Datenschutzaufsichtsbehörde, soweit personenbezogene Daten betroffen sind.
- BNetzA und BfDI arbeiten kooperativ; BfDI unterstützt in Datenschutzfragen.
- Erfordert ein BNetzA-Verfahren die Prüfung personenbezogener Datenverarbeitung, wird der BfDI beteiligt.
- BNetzA ist an das Ergebnis der BfDI-Prüfung gebunden; Datenschutz-Geldbußen nach Art. 40 Abs. 4 DA liegen beim BfDI.

3 | Bußgelder: Höhe und Fokus

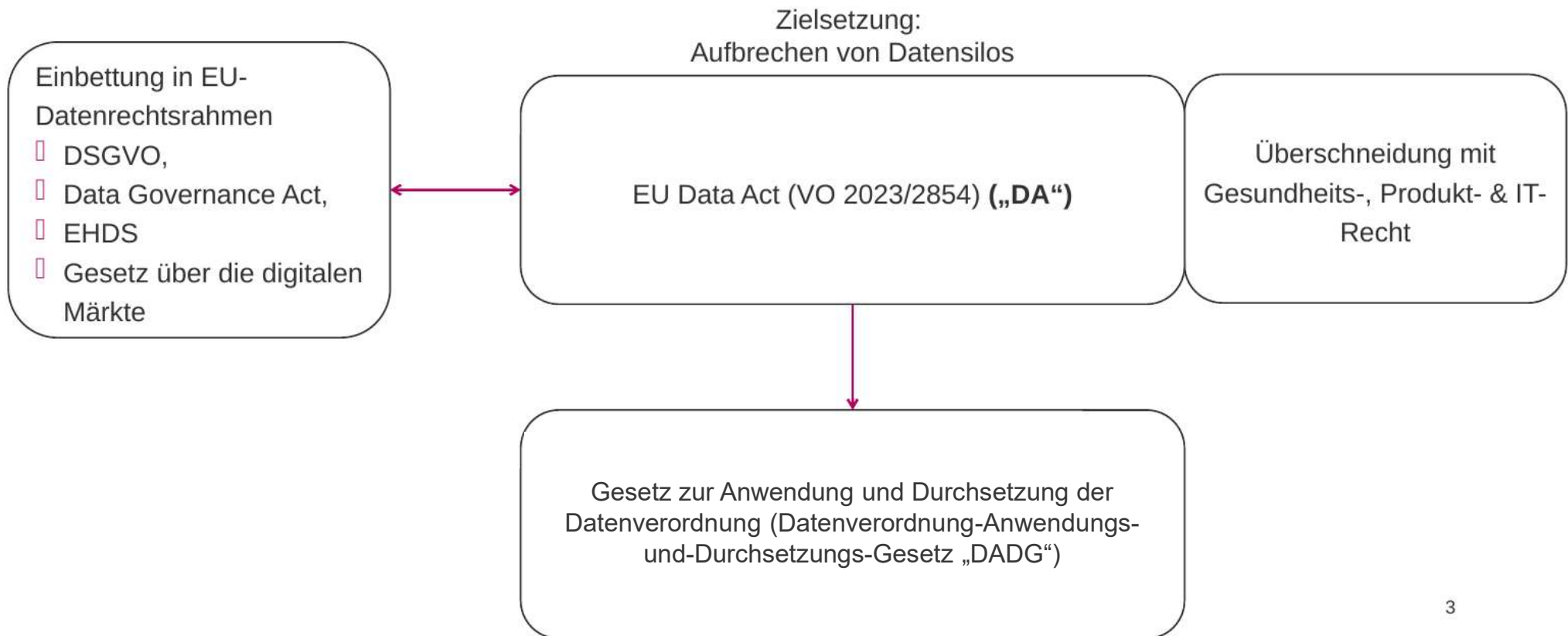
- Bis 5 Mio. EUR / 2 % Weltumsatz*: Nutzer zur Datenbereitstellung auffordern oder durch geschäftliche Anreize dazu veranlassen (Torwächter; Art. 5 Abs. 3 Buchst. a/b DA).

Merke: Die BNetzA ist die zentrale Data-Act-Durchsetzungsbehörde; personenbezogene Daten bleiben fachlich bei der Datenschutzaufsicht.

Quelle: DADG, §§ 1–16.

Rechtsrahmen

Der EU Data Act als Ausgangspunkt nationaler Umsetzung, paralleler Geltung und regulatorischer Überschneidung



Rechtsrahmen

Verhältnis EHDS – Data Act / Beispielsfall

Ausgangslage: Ein Krankenhaus nutzt ein vernetztes Herzmonitoring-System, das Vitaldaten von Patienten kontinuierlich erfasst und an den Hersteller übermittelt. Die Geräte werden gemietet.



Rechtsrahmen

Verhältnis EHDS – Data Act

Aspekt	EHDS	EU Data Act
Regelungscharakter	Sektorspezifischer Rechtsrahmen für Gesundheitsdaten	Horizontaler, sektorübergreifender Rechtsrahmen
Gegenstand	Elektronische Gesundheitsdaten, (Primär- & Sekundärnutzung)	Produkt- und Dienstdaten, v.a. aus vernetzten Produkten
Adressaten	Patienten, Gesundheitsdienstleister, Forschung, Behörden	Nutzer, Dateninhaber, Dritte
Zugangsmodell	Systemisch/behördlich geregelter Zugang zu Gesundheitsdaten (EHR-basiert)	Rechtsanspruch auf direkten Datenzugang zwischen privaten Parteien
Umfang des Datenzugangs	Zugang zu großen Datenbeständen, inkl. Metadaten und Daten, die von Dritten bereitgestellt wurden	Zugang ausschließlich zu den Daten des vom Nutzer verwendeten vernetzten Produkts bzw. verbundenen Dienstes
Typischer Datenfluss	Antrag → öffentliche Stelle (HDAB) → Zugang zu Gesundheitsdaten (Datenaustausch erfolgt über sog. Electronic-Health-Record Systeme)	Antrag Nutzer → Dateninhaber → ggf. Dritter

Rechtsrahmen

Verhältnis EHDS – Data Act / Beispielsfall

	Zugang nach EHDS	Zugang nach EU Data Act
Wer fordert an?	z.B. Ein universitäres Forschungsinstitut.	Das Krankenhaus als Nutzer der vernetzten Medizinprodukte.
Welche Daten?	Große Mengen strukturierter Gesundheitsdaten aus elektronischen Patientenakten (EHR), einschließlich Metadaten und Daten, die von vielen Krankenhäusern bereitgestellt wurden.	Ausschließlich die Produkt- und Nutzungsdaten, die durch die vom Krankenhaus genutzten Geräte erzeugt werden (z. B. Messwerte, Nutzungsdauer, Gerätestatus).
Datenherkunft	Von Gesundheitsdateninhabern iSd. EHDS	Dateninhaber iSd. Data Act
Wie erfolgt der Zugang?	Anfrage bei zuständiger Behörde (HDAB)	Anfrage bei Dateninhaber.
Zugangsvoraussetzung	Primär- oder Sekundärnutzung nach EHDS (z.B. Forschungszwecke)	Dateninhaber verarbeitet Daten des Nutzers

II

Ist mein Medizinprodukt ein vernetztes Gerät oder ein verbundener Dienst im Sinne des Data Act?

Produktabgrenzung, technische Tatbestandsmerkmale und MedTech-Beispiel.

II. Ist mein Produkt ein vernetztes Produkt oder ein verbundener Dienst?

Abgrenzung anhand der BNetzA-Factsheets – mit einem Beispiel für jede Kategorie

Faustformel: Das vernetzte Produkt erzeugt und übermittelt Daten; der verbundene Dienst ist die damit verknüpfte Software und kann die Funktionsweise beeinflussen.

Vernetztes Produkt



Beispielgrafik

Physisches Gerät mit Datenerfassung und Datenübermittlung

Definition

Gegenstand, der Daten über Nutzung, Leistung oder Umgebung erfasst und sie über einen kabelbasierten oder kabellosen Zugang übermitteln kann.

Beispiel aus dem Factsheet

Smartwatch (genannt unter „smarte Elektronik“).

Praxisnahe Einordnung

Für MedTech besonders anschlussfähig sind Wearables bzw. andere vernetzte Medizin- und Gesundheitsgeräte.

Verbundener Dienst



Mit dem Produkt verbundene Software mit Einfluss auf die Funktionsweise

Definition

Mit einem vernetzten Produkt verbundene Software, die Daten oder Befehle übermittelt und dadurch die Funktionsweise des Produkts beeinflussen kann.

Beispiel aus dem Factsheet

App zur Steuerung der Lichteinstellungen oder der Temperatur eines smarten Kühlschranks.

Praxisnahe Einordnung

Übertragbar auf Companion-Apps oder Hersteller-Software, die ein Gerät steuert, konfiguriert oder Funktionen freischaltet.

Was ist ein vernetztes Produkt?

- bezeichnet „einen **Gegenstand**, der **Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt** und der **Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann** und dessen **Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist**“ (Art. 2 Nr. 5 DA).

➤ **Frage:** Handelt es sich bei folgendem Beispiel um ein *vernetztes Produkt* im Sinne des EU Data Act?

Beispielfall: Ein vernetztes medizinisches Überwachungsgerät (z. B. ein tragbarer EKG-Monitor) misst kontinuierlich Vitalparameter des Patienten und übermittelt diese drahtlos an ein System des Herstellers.

Das Gerät erzeugt sowohl Mess- und Nutzungsdaten als auch Darstellungen und Berichte für medizinisches Fachpersonal.

Was ist ein vernetztes Produkt?

- **Gegenstand** (weit auszulegen): Erfasst sind sämtliche beweglichen und unbeweglichen Gegenstände, einschließlich Infrastrukturen wie Satellitennetze; eine Beschränkung auf rein körperliche Güter besteht nicht (vgl. ErwG 14 Data Act).
 - Tragbarer EKG-Monitor = Gegenstand i.S.d. Art. 2 Nr. 5 DA
- **Erlangen, Generieren oder Erheben von Daten über seine Nutzung oder Umgebung:**
hier **Daten** = „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material;“ (Art. 2 Nr. 1 DA).
 - Tragbarer EKG-Monitor erhebt u.a. Vitalparameter (z.B. Herzfrequenz, Rhythmus). Diese Informationen sind als Daten i.S.d. Art. 2 Nr. 1 DA anzusehen.

Was ist ein vernetztes Produkt?

- **Übermittlung von Produktdaten:**

- Übermittlung erfolgt über elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang.

➤ EKG-Monitor: drahtlose Übertragung an Backend des Herstellers

- **Produktdaten:** „Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können;“ (Art. 2 Nr. 15 DA)

➤ Bei EKG-Monitor Abrufen (Übermitteln) von generierten, erhobenen Daten konzeptionell vorgesehen

Was ist ein vernetztes Produkt?

Übermittlung von Produktdaten:

Datenkategorie	Produktdaten – allgemein	Beispiel: Tragbarer EKG-Monitor
Durch Nutzung generierte Daten	Daten entstehen durch den Betrieb und die Nutzung des vernetzten Produkts (Art. 2 Nr. 15 DA).	EKG-Mess- und Zustandsdaten entstehen durch das Tragen und Verwenden des Monitors.
↳ Art der Datenerzeugung	Absichtlich aufgezeichnete oder indirekt durch Nutzungshandlungen generierte Daten.	Aktive Herzaktivitätsmessung sowie passive Datengenerierung während des Betriebs.
↳ Bezug	Daten über Nutzung oder Umgebung des Produkts.	Herzaktivität, Tragezustand, Bewegung, Umfeldbedingungen.
↳ Roh- (Primär-) und einfach aufbereitete Daten	Erfasst sind Rohdaten sowie einfach aufbereitete Daten , soweit diese ohne wesentliche Zusatzinvestitionen nutzbar sind; inkl. Metadaten und Zeitstempeln .	EKG-Rohsignale, vorverarbeitete Kurven, Zeitstempel, Messdauer,
↳ Typische Beispiele	Sensordaten, UI-Daten, Status- und Diagnosedaten (z. B. Batteriestand).	Batteriestand, Elektrodenkontakt, Fehlermeldungen, Standby-Status.
Nicht erfasst (Abgrenzung)	Abgeleitete oder gefolgerte Informationen , insbesondere auf Basis proprietärer Algorithmen, sind ausgeschlossen.	Ärztliche Befunde, Handlungsempfehlungen, Arrhythmie-Bewertungen.

Was ist ein vernetztes Produkt?

- *Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer –*

➤ Bei einem tragbaren EKG-Monitor erfolgt die Verarbeitung und Übertragung im Interesse des Nutzers (Patienten) sodass die Negativvoraussetzung erfüllt ist und ein *vernetztes Produkt* gem. Art. 2 Nr. 5 DA vorliegt.

Praxishinweis:

- Übergangsfrist bis zum **12. September 2026** für Pflichten zur Gestaltung vernetzter Produkte und verbundener Dienste nach Art. 3 Abs. 1 DA



Accessibility by Design: Anforderungen an die Konzeption des Produkts

Zugang durch Access by Design und anschließender Zugangsanspruch.

III. Accessibility by Design

Meisterernst

Rechtsanwälte

Datenzugang muss in Produkt- und Softwarearchitektur mitgedacht werden

Art. 3 Data Act verlangt keinen reinen „Exportknopf“ am Ende – sondern eine Architektur, die Datenzugang standardmäßig einfach, sicher und maschinenlesbar ermöglicht.



Vernetztes Monitoring-Gerät + Companion-App

Beispielhafte Umsetzung: Im Nutzerkonto ist früh sichtbar, welche Produkt- und Dienstdaten entstehen; der Export oder API-Zugriff ist sicher, strukturiert und maschinenlesbar vorgesehen.

Was früh im Design zu lösen ist

1 Zugang

Daten müssen grundsätzlich leicht, sicher, kostenfrei, vollständig, strukturiert, gängig und maschinenlesbar verfügbar sein.

2 Transparenz

Vor Vertragsschluss sind u. a. Art, Format, Umfang, Echtzeitfähigkeit und Zugangsweg der Daten klar zu erläutern.

3 MedTech-Schutz

Schnittstellen nicht isoliert bauen: Datenschutz, Geschäftsrisiko, Cybersecurity und Produktsicherheit mitprüfen.

Fazit: Access-by-Design ist ein Produkt-, IT- und Rechtsprojekt – nicht nur eine spätere Vertrags- oder Supportfrage.

Datenzugang für Nutzer

Zugang durch Access by Design, Art. 3 DA

- Vernetzte Produkte und verbundene Dienste *sollen* so konzipiert sein, dass Produktdaten und verbundene Dienstdaten für den Nutzer direkt zugänglich sind (Access by Design)
- Die Daten sind dem Nutzer in einer geeigneten, strukturierten und gängigen Form zur Verfügung zu stellen.
- **Abgrenzung:** Der Zugang nach Art. 3 DA erfasst Produktdaten, nicht jedoch „Inhalte“ im Sinne des Art. 1 Abs. 2 lit. a) DA.

Datenzugang für Nutzer

“Produktdaten“ vs. „Inhalte“

Abgrenzung: Inhalte vs. Daten – Beispiele

Inhalte



Smart-TV

- Audiovisuelle Inhalte (Film, Serie)
- Ergebnis eines kreativen Prozesses
- Kein Zugang nach Kapitel II
(Art. 1 Abs. 2 lit. a DA)



Inhalte – kein Zugang
(Art. 1 Abs. 2 lit. a DA)

Daten (Digitale Kamera)



Produkt- & Sensordaten – Zugangspflichtig

- Produkt- und Sensordaten
- Nicht-kreativ, technisch erzeugt
- Zugangspflicht nach Kapitel II
(Art. 3–5 DA)

**Produkt- & Sensordaten –
Zugangspflichtig**
(Kapitel II DA)



Datenzugang für Nutzer

Zugang durch Access by Design, Art. 3 DA

- Nutzer (Art. 2 Nr. 12 Data Act): besitzt oder hat zeitweiliges Nutzungsrecht an vernetztem Produkt



SGB V-Interoperabilität (§ 374a) und Data Act

Gemeinsamkeiten, Unterschiede und Fazit für doppelt betroffene Hersteller

Drei Punkte für die Einordnung

1 Gemeinsamkeit

- Beide Regime zielen auf nutzbare Daten aus digital vernetzten Produkten bzw. Diensten.
- Beide verlangen technisch beherrschbare, sichere und interoperable Datenflüsse.
- In der Produktentwicklung gehören Schnittstelle, Datenformat und Security daher zusammen.

2 Nutzerbezug ≠ identisch

- SGB V: Versicherter; Daten sollen auf Einwilligungsbasis in eine gelistete DiGA übertragen werden.
- Data Act: Nutzer kann Daten selbst erhalten oder Weitergabe an Dritte verlangen.
- Die Rollenlogik ist deshalb ähnlich, aber nicht deckungsgleich.

3 Eingriffsrichtung ≠ identisch

- SGB V: Übermittlung in die DiGA; Beeinflussung des Hilfsmittels oder Implantats durch die DiGA ist unzulässig.
- Data Act: Zugang und Weitergabe von Produkt- und Dienstdaten; kein spezifisches DiGA-Schnittstellenregime.
- Data-Act-Konformität ersetzt § 374a SGB V nicht – und umgekehrt.

Fazit

Wenn ein Unternehmen sowohl § 374a SGB V als auch dem Data Act unterfällt, sollten Schnittstellen, Datenmodelle, Einwilligung/DSGVO, Security und Produktregulierung gemeinsam geplant werden.

IV

Recht auf Datenzugang und Pflicht zur Datenbereitstellung gegenüber Nutzern und Dritten; vertragliche Gestaltungsmöglichkeiten und Schutz von Geschäftsdaten

Nutzerzugang, Drittweitergabe, Vertragsbeziehungen, Klauselkontrolle und Geschäftsgeheimnisse.

Datenzugang für Nutzer

Anspruch auf Zugang, Art. 4 DA

- Für den Fall, dass Voraussetzungen für einen Zugang nach Art. 3 Abs. 1 DA nicht geschaffen wurden, enthält Art. 4 Abs. 1 einen kostenlosen **Zugangsanspruch** des Nutzers gegenüber den Dateninhaber.
- Beschränkt auf
„*ohne Weiteres verfügbare Daten*“ Produktdaten und verbundene Dienstdaten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, wobei über eine einfache Bearbeitung hinausgegangen wird (Art. 2 Nr. 17 DA):

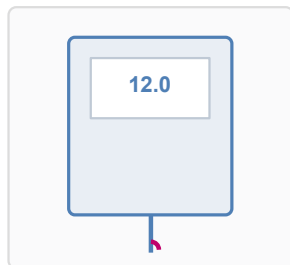
→ z.B. Rohdaten oder aufbereitete Daten
- **Nicht erfasst** sind Daten, die bei der Nutzung entstehen, aber nicht dafür ausgelegt sind, außerhalb der Komponente oder des Produkts gespeichert oder übermittelt zu werden.

Accessibility by Design: Daten entstehen – sind aber nicht „ohne Weiteres verfügbar“

Meisterernst
Rechtsanwälte

Entscheidend: „ohne Weiteres verfügbare Daten“ kann der Dateninhaber ohne unverhältnismäßigen Aufwand über eine einfache Handlung erlangen (Art. 2 Nr. 17 Data Act).

Beispiel 1: Infusionspumpe



Vernetzte
Infusionspumpe

Daten entstehen

Interne Regelungs- und Sensordaten werden während der Dosierung erzeugt.

Aber nicht ohne Weiteres verfügbar

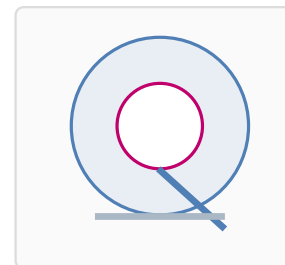
Beispiel: Werte werden nur flüchtig im Steuerungsmodul verarbeitet und weder gespeichert noch nach außen übertragen.

Folge

Der Data Act verlangt nicht, erst eine neue zentrale Speicherung dieser Daten einzubauen.

Daten entstehen – aber nicht bereits deshalb „ohne Weiteres verfügbar“.

Beispiel 2: Bildgebungssystem



Vernetztes
Bildgebungssystem

Daten entstehen

Detektoren erzeugen Rohsignale; Software verarbeitet sie zum medizinisch nutzbaren Bild.

Aber nicht ohne Weiteres verfügbar

Beispiel: Zwischenwerte bleiben innerhalb einer Verarbeitungskomponente und sind nicht als abrufbarer Datenbestand ausgelegt.

Wichtig

Abrufbare Roh- oder vorverarbeitete Daten können dagegen erfasst sein; abgeleitete Informationen aus komplexen proprietären Algorithmen sind grundsätzlich ausgenommen.

Daten entstehen – aber nicht bereits deshalb „ohne Weiteres verfügbar“.

Fazit: „Daten werden generiert“ ≠ „alle Daten müssen bereitgestellt werden“. Zu prüfen sind Abrufbarkeit, technischer Aufwand und Verarbeitungsstufe.

Quelle: Art. 2 Nr. 15–17, Art. 3 Data Act; Erwägungsgründe 15 und 20; EU-Kommission, Guidelines on Data Act definitions (2025).

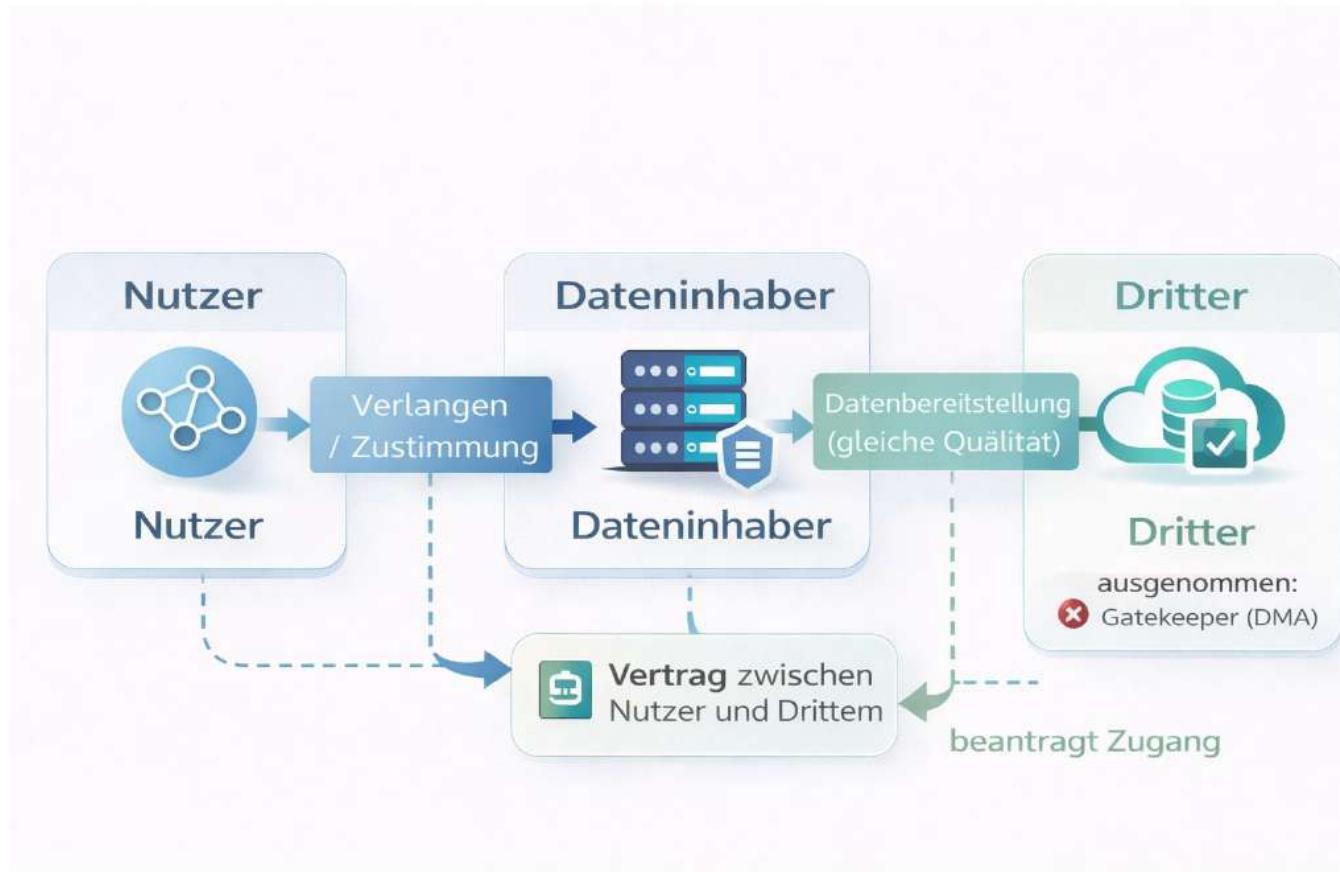
Datenzugang für Nutzer

“Produktdaten“ vs. „Inhalte“

- Nicht vom Anwendungsbereich Kapitel II (und damit nicht von Art. 3 und Art. 4 D) erfasst, sind sog. „Inhalte“ i.S.d. Art. 1 Abs. 2 lit. a) DA :
 - Textliche, auditive oder audiovisuelle Informationen
 - Ergebnis eines kreativen Prozesses
 - Für menschliche Wahrnehmung oder Konsum bestimmt
 - Häufig durch Urheber- oder IP-Rechte geschützt

Datenzugang Dritter

Zugang für Datenempfänger bzw. Dritte, Art. 5 DA



Datenzugang

Konflikt Geschäftsgeheimnisse

- **Grundkonflikt:** Data Act verpflichtet zum Datenzugang – Schutz von Geschäftsgeheimnissen bleibt zulässig, aber eingeschränkt.
- **Schutz als Regel, Verweigerung als Ausnahme:** Datenzugang ist grundsätzlich zu gewähren, unter angemessenen technischen und organisatorischen Schutzmaßnahmen(Art. 4 Abs. 6, 7; Art. 5 Abs. 9, 10 DA).
- **Zugangsverweigerung nur ultima ratio:** Nur bei hoher Wahrscheinlichkeit eines schweren wirtschaftlichen Schadens durch Offenlegung(Art. 4 Abs. 8; Art. 5 Abs. 11 DA).
 - Mitteilung an Behörde erforderlich

Mitteilung zur „Geschäftsgeheimnis-Handbremse“**Geschäftsgeheimnis-Handbremse – Mitteilungen nach Art. 4 (7), (8) oder Art. 5 (10), (11) Data Act**

Der Data Act sieht mit der „Handbremse für Geschäftsgeheimnisse“ einen Mechanismus zum Schutz von Geschäftsgeheimnissen vor. Dieser Mechanismus gibt Bedingungen vor, unter denen ein Dateninhaber in Ausnahmefällen die Weitergabe von Geschäftsgeheimnissen aussetzen oder verweigern kann. Die Entscheidung des Dateninhabers ist ordnungsgemäß zu begründen und dem Nutzer bzw. Dritten unverzüglich schriftlich mitzuteilen.

Sofern ein objektiver Nachweis dafür erbracht wird, dass die Offenlegung von Geschäftsgeheimnissen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden zur Folge hätte, können Dateninhaber ein Datenverlangen im Einzelfall für die betroffenen Daten auch ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, insbesondere der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen und dem Nutzer bzw. Dritten unverzüglich schriftlich vorzulegen.

Dateninhaber sind verpflichtet der Bundesnetzagentur mitzuteilen, sofern sie den Datenzugang gemäß Art. 4 (7), (8) oder Art. 5 (10), (11) Data Act verweigern. Nutzen Sie für diese Mitteilungen bitte das nachfolgende Formular.

Felder mit * sind zwingend auszufüllen.

Haben Sie von der „Geschäftsgeheimnis-Handbremse“ Gebrauch gemacht und die Herausgabe von Geschäftsgeheimnissen gemäß Artikel Art. 4 (7), (8) oder Art. 5 (10), (11) Data Act verweigert oder ausgesetzt bzw. ein Datenzugangsverlangen abgelehnt?*

- ☐ Ja, die Herausgabe von Geschäftsgeheimnissen wurde ausgesetzt (Art. 4 (7); Art. 5 (10))
- ☐ Ja, die Herausgabe von Geschäftsgeheimnissen wurde verweigert (Art. 4 (7); Art. 5 (10))
- ☐ Ja, ein Datenzugangsverlangen wurde abgelehnt (Art. 4 (8); Art. 5 (11))
- ☐ Nein

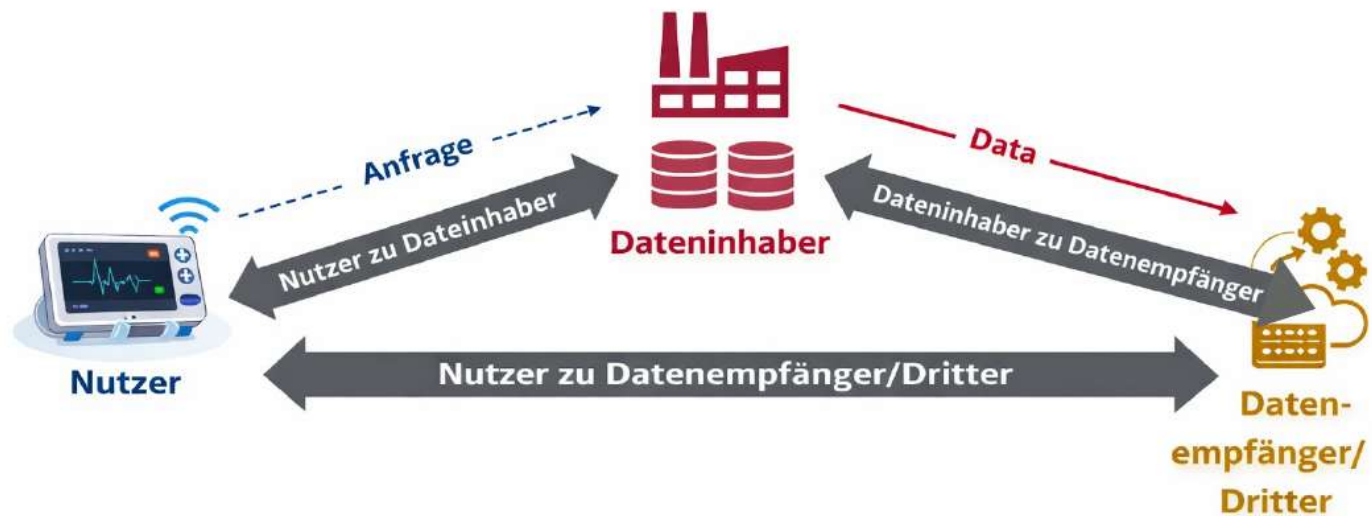
Datenzugang

Konflikt Geschäftsgeheimnisse

- **Praktischer Lösungsansatz:** Mittelweg zwischen gesetzlicher Zugangspflicht und Schutz von Geschäftsgeheimnissen
- 1) Identifikation:** welche Daten stellen Geschäftsgeheimnissen dar, ggf. auch erst in Kombination
 - 2) Absicherung:** Primärer Schutz über technische, organisatorische und vertragliche Maßnahmen.
 - technische Maßnahmen (z. B. Zugriffsbeschränkungen, Schnittstellenkontrolle),
 - organisatorische Maßnahmen (z. B. Rollen- und Berechtigungskonzepte),
 - vertragliche Absicherungen (z. B. Vertraulichkeits- und Nutzungsbeschränkungen).
 - 3) Verweigerung:** wenn Schutzmaßnahmen nicht ausreichen oder vom Datenempfänger verweigert werden

Vertragsgestaltung

Übersicht der Vertragsbeziehungen



Vertragsgestaltung

Beziehung Nutzer / Dateninhaber

	Vertrag zum Datenzugang des Nutzers	Datenlizenzvertrag
Zweck	Durchsetzung des gesetzlichen Zugangsanspruchs des Nutzers	Nutzung nicht-personenbezogener Daten durch den Dateninhaber
Rechtsgrundlage	Art. 3 und Art. 4 Data Act	Art. 4 Abs. 13 Data Act
Rechtsnatur	Gesetzlicher Anspruch, nicht dispositiv	Erforderlich, wenn der Dateninhaber Daten selbst nutzen will
Vertragliche Einbettung	Kann in einem Hauptvertrag geregelt werden	Teil von Kauf-, Miet- oder Leasingvertrag (kein Kopplungsverbot)
Regelungsinhalt	Zugangsmodalitäten, Formate, Fristen, Schutzmaßnahmen	Zweckbindung, Nutzungsumfang, Ausforschungsverbote
Zulässige Einschränkungen	Einschränkung grds. nur bei Geschäftsgeheimnissen (Art. 4 Abs. 7, 8 DA)	Nutzung nur wie vereinbart; gewerbliche Position des Nutzers nicht schädigen
Schranken	Zugang darf nicht unangemessen erschwert werden (Art. 4 Abs. 4 DA)	Weitergabe Nicht-personenbezogener Produktdaten nur zur Vertragserfüllung mit dem Nutzer (Art. 4 Abs. 14 DA)

Vertragsgestaltung

Beziehung zwischen Nutzer und Datenempfänger (Dritter)

- **Weiter Gestaltungsspielraum des Nutzers:**
 - Keine zu Art. 9 DA vergleichbare Regelung zur Gegenleistung. Nutzer ist frei, Gegenleistung zu verhandeln.
 - **Zweck- und vertragsgebundene Datennutzung:**
Nutzer obliegt Zweck der Datennutzung zu vereinbaren (Art. 6 Abs. 1 DA)
 - **Keine Erweiterung der Zugriffsrechte für Dritte durch Vertrag:**
Vereinbarungen zwischen Nutzer und Drittem, die über Zugangsrecht des Nutzers hinausgehen, binden den Dateninhaber nicht
- **Schutz der Nutzerrechte**
nicht Wahlmöglichkeiten des Nutzers untergraben oder beeinträchtigen (Art. 6 Abs. 2 lit. a) DA).
- **Weitergabefreiheit des Nutzers**
Nutzer darf nicht daran gehindert werden, die Daten weiterzugeben (Art. 6 Abs. 2 lit. h) DA).

Vertragsgestaltung

Beziehung Dateninhaber / Datenempfänger (Dritte)

- Über die Datenbereitstellung ist ein Vertrag zu schließen (Art. 8 Abs. 1 DA).
- Grundsätzliche Vertragsbedingungen:
 - Bereitstellung hat zu „fairen, angemessenen, und nichtdiskriminierenden Bedingungen“ zu erfolgen (Art. 8 Abs. 1 DA).
 - Keine Dispositionshoheit des Dateninhabers über Zweck der Nutzung; diese liegt bei Nutzer (vgl. Art. 6 DA).
- Gegenleistung / Marge des Dateninhabers für Datenbereitstellung darf „diskriminierungsfrei und angemessen“ vereinbart werden (Art. 9 DA):
 - Angemessenheit wird in Art. 9 Abs. 2, 3 DA konkretisiert (z.B. Berücksichtigung angefallener Kosten für Bereitstellung, Investitionen in die Erhebung und Generierung von Daten sowie Umfang, Format und Art der Daten).
- Weitere Pflichten des Datenempfängers: Kein Wettbewerbsgebrauch, keine Weitergabe an Torhüter, Wahrung von Sicherheit (Art. 6 DA).

Vertragsgestaltung

Klauselkontrolle bei AGB

- **Zwingende Klauselkontrolle (B2B):** Verbot missbräuchlicher datenbezogener Vertragsklauseln – nicht abdingbar (Art. 13 Abs. 1, 9 DA)
- **Anwendungsbereich:** Erfasst datenbezogene Klauseln zwischen Unternehmen (Datenzugang, Datennutzung, Haftung, Rechtsbehelfe)
- **Einbeziehungskontrolle** (Einseitig auferlegte Klauseln): Kontrolle greift, wenn Klauseln nicht real verhandelbar waren (Art. 13 Abs. 6 DA)

Vertragsgestaltung

Klauselkontrolle bei AGB

- **Inhaltskontrolle:** „Schwarze Liste“ (Art. 13 Abs. 4) unwiderlegbar missbräuchlich:

„Eine Vertragsklausel gilt insbesondere dann als missbräuchlich im Sinne des Absatzes 3, wenn sie Folgendes bezweckt oder bewirkt:

- a) den Ausschluss oder die **Beschränkung der Haftung** der Partei, die die **Klausel einseitig auferlegt** hat, für **vorsätzliche oder grob fahrlässige** Handlungen;
- b) den **Ausschluss der Rechtsbehelfe**, die der Partei, der die Klausel **einseitig auferlegt wurde**, bei Nichterfüllung von Vertragspflichten zur Verfügung stehen, oder den Ausschluss der Haftung der Partei, die die Klausel einseitig auferlegt hat, bei einer Verletzung dieser Pflichten;
- c) das ausschließliche Recht der Partei, die **die Klausel einseitig auferlegt** hat, zu bestimmen, **ob die gelieferten Daten vertragsgemäß sind**, oder Vertragsklauseln auszulegen.“

Vertragsgestaltung

Klauselkontrolle bei AGB

- **Inhaltskontrolle: „Graue Liste“** (Art. 13 Abs. 5) widerlegbar missbräuchliche Klauseln:

Eine Vertragsklausel gilt als missbräuchlich im Sinne des Absatzes 3, wenn sie Folgendes bezweckt oder bewirkt:

- a) eine **unangemessene Beschränkung der Rechtsmittel** bei Nichterfüllung von Vertragspflichten oder der Haftung bei einer Verletzung dieser Pflichten oder eine Erweiterung der Haftung des Unternehmens, dem die Klausel einseitig auferlegt wurde;
- b) das Recht der Partei, die die Klausel einseitig auferlegt hat, **auf Zugang zu Daten** der anderen Vertragspartei und deren Nutzung in einer Weise, die den berechtigten Interessen der anderen **Vertragspartei erheblich schadet, insbesondere**, wenn diese Daten **sensible Geschäftsdaten** enthalten oder durch das Geschäftsgeheimnis oder durch Rechte des geistigen Eigentums geschützt sind;
- c) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, daran, die von ihr **während der Vertragslaufzeit bereitgestellten oder generierten Daten zu nutzen**, oder eine Beschränkung der Nutzung dieser Daten insofern, als diese Partei nicht berechtigt ist, diese Daten in angemessener Weise zu nutzen, zu erfassen, darauf zuzugreifen oder sie zu kontrollieren oder zu verwerten;
- d) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, daran, die Vereinbarung innerhalb einer **angemessenen Frist zu kündigen**;
- e) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, daran, während der Vertragslaufzeit oder innerhalb einer angemessenen Frist nach Kündigung des Vertrags eine **Kopie der von ihr bereitgestellten oder generierten Daten zu erhalten**;
- f) die Möglichkeit, dass die Partei, die die Klausel einseitig auferlegt hat, den Vertrag mit unangemessen kurzer Frist kündigen darf, und zwar unter Berücksichtigung jeglicher realistischer Möglichkeit für die andere Vertragspartei, zu einem anderen, vergleichbaren Dienst zu wechseln, und des durch die Kündigung verursachten finanziellen Nachteils, außer bei Vorliegen schwerwiegender Gründe;
- g) die Möglichkeit, dass die Partei, die die Klausel einseitig auferlegt hat, **den vertraglich vereinbarten Preis oder eine andere wesentliche Bedingung in Bezug auf Art, Format, Qualität oder Menge der weiterzugebenden Daten ohne eine im Vertrag spezifizierte stichhaltige Begründung wesentlich abändert**, ohne dass der anderen Partei das Recht eingeräumt wird, den Vertrag im Falle einer solchen Abänderung zu kündigen.

Vertragsgestaltung

Klauselkontrolle bei AGB

- **Inhaltskontrolle:** Allgemeine Missbrauchskontrolle (Art. 13 Abs. 3 DA)

„Vertragsklauseln sind missbräuchlich, wenn ihre Anwendung eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt oder gegen das Gebot von Treu und Glauben verstößt.“

- **Rechtsfolge & Praxis:** Nur die missbräuchliche Klausel ist unwirksam; Mustervertragsklauseln sollen Orientierung geben (ErwG 62 DA)
- **Zeitliche Anwendung:**
 - Ab 12.09.2025 für neue Verträge
 - Ab 12.09.2027 auch für Altverträge (Art. 50 DA), wenn
 - unbefristet oder
 - Laufzeit ≥ 10 Jahre ab 11.01.2024

Rechtsschutz

- **Beschwerderecht**

- Allgemeines Beschwerderecht bei Verstößen gegen den Data Act (Art. 38 DA)
- Besondere Beschwerdemöglichkeit: Beschwerde bei Verweigerung des Datenzugangs durch den Dateninhaber (Art. 4 Abs. 3 DA)
- - Bundesnetzagentur zuständige Behörde nach § 2 Abs. 2 Nr. 1 DADG

IA

- **Rechtsbehelfe:** Anspruch auf wirksamen gerichtlichen Rechtsbehelf gegen

- Rechtsverbindliche Entscheidungen der zuständigen Behörde (Art. 39 Abs. 1 DA)
- Ausbleibende Bearbeitung einer Beschwerde durch zuständige Behörde (Art. 39 Abs. 2 DA)

- **Sanktionen:** Verhängung von Geldbußen und weiteren Sanktionen bei Verstößen (Art. 40 Abs. 4 DA)

Nach § 15 DADG: BNetzAgentur grds. zuständig für Bußgelder wegen Verstoßes gegen DA

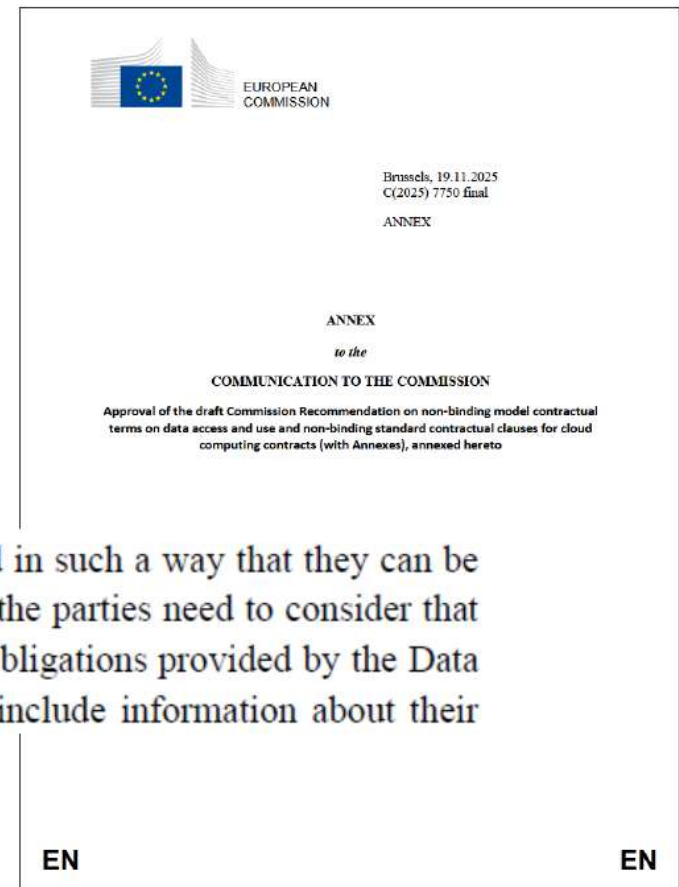
Nach § 16 DADG: Zuständigkeit BfDI soweit Verstoß personenbezogen Daten betrifft

Checkliste: Ist mein Produkt schon “Data Act“ ready?

O Mustervertragsbedingungen für Datenaustauschverhältnisse

(vgl. *ANNEX to the COMMUNICATION TO THE COMMISSION
Approval of the draft Commission Recommendation on non-binding
model contractual terms on data access and use and non-binding
standard contractual clauses for cloud computing contracts (with
Annexes), annexed hereto, 19.11.2025*)

The MCTs and SCCs are nonbinding. They are and have been drafted in such a way that they can be adapted by the parties according to their contractual needs. However, the parties need to consider that these MCTs and SCCs were drafted to be in line with the rights and obligations provided by the Data Act and were also designed to be consistent with each other. They include information about their



V

Anforderungen beim Wechsel zwischen Datenverarbeitungsdiensten

Wechselvoraussetzungen, Vertragsgestaltung und technische Anforderungen.

Nicht jede cloudbasierte Komponente ist bereits ein Datenverarbeitungsdienst i. S. v. Art. 2 Nr. 8 Data Act. Entscheidend ist, ob der konkrete Dienst einen bedarfsgesteuerten Netzzugang zu einem gemeinsam genutzten Pool skalierbarer und elastischer Rechenressourcen ermöglicht.

Datenverarbeitungsdienste – Kapitel VI: Anbieterwechsel

- Kapitel VI betrifft Anbieter von Datenverarbeitungsdiensten und deren Kunden – insbesondere typische IaaS-, PaaS- und SaaS-Modelle.
- Anbieter müssen Hindernisse für den Wechsel zu einem anderen Anbieter, die Rückführung in eigene Infrastruktur und parallele Nutzung beseitigen.
- Verträge müssen Wechselablauf, Datenexport, Kündigung und Unterstützung transparent regeln.
- Ab 12. Januar 2027 dürfen keine Wechselentgelte mehr erhoben werden.

VI

Übergangsfristen für die Produktumstellung

Geltungsbeginn, Produktstichtage, Altverträge, Simplification und Readiness-Check.

Zeitlicher Anwendungsrahmen: 12.09.2025, 12.09.2026 und 12.09.2027

GELTENDES RECHT

- Der Data Act gilt grundsätzlich seit 12. September 2025.
- Art. 3 Abs. 1 („by design“) gilt für vernetzte Produkte und verbundene Dienste, die nach dem 12. September 2026 in Verkehr gebracht werden.
- Kapitel IV gilt für nach dem 12. September 2025 geschlossene Verträge; bestimmte Altverträge werden ab 12. September 2027 erfasst.
- Für den Vortrag am 17. September 2026 ist daher vor allem der neue Produktstichtag des Art. 3 Abs. 1 praktisch relevant.

Praxishinweis: Geltungsbeginn des Data Act und zeitliche Anwendbarkeit einzelner Pflichten strikt trennen.

Quelle: VO (EU) 2023/2854, Art. 50

Geschäftsgeheimnisse

Simplification / geplante Änderungen zur Stärkung des Geschäftsgeheimnisschutzes

Geplante Änderung der Art. 4 Abs. 8, Art. 5 Abs. 11 DA

Meisterernst

Rechtsanwälte

Data-Act derzeitige Fassung

Bedingungen für Verweigerung

(Art. 4 (8) § Art. 5 (11) DA):

Trotz techn./orga. Maßnahmen besteht

hohe Wahrscheinlichkeit, dass
schwerer wirtschaftlicher Schaden
durch Offenlegung verursacht wird



Verweigerung des Zugangs
ggü. einem **Nutzer**
(Art. 4 Abs. 8 DA)



Verweigerung des Zugangs
ggü. einem **Dritten**
(Art. 5 Abs. 11 DA).

Digital-Omnibus Entwurf



Verweigerung des Zugangs
ggü. einem Nutzer oder
Dritten wenn trotz
techn./org. Maßnahmen
eines **Dritten** hohe
Wahrscheinlichkeit besteht,
dass bei Offenlegung von
Geschäftsgeheimnissen ein
schwerer wirtschaftlicher
Schadeneintritt.



Verweigerung des Zugangs
ggü. einem Nutzer oder
Dritten wenn **Offenlegung**
von Geschäftsgeheimnissen
ggü. Nutzer hohes Risiko
des rechtswidrigen Erwerbs,
der rechtswidrigen Nutzung
oder der Offenlegung ggü.
Einrichtungen in Drittländern
birgt.

**Zusätzlicher Verweigerungsgrund in Art. 4 Abs. 8⁵ und Art.
5 Abs. 11 DA mit aufgenommen**

Checkliste: Ist mein Produkt schon “Data Act“ ready?*

1. Vernetztes Produkt?

einen Gegenstand.

- der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt
- und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann
- und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist (Art. 2 (5) Data Act);

2. Datenzugang für Nutzer

☐ Werden alle vom Gerät erzeugten „ohne Weiteres“ verfügbare Daten identifiziert? (Art. 2 Nr. 17 Data Act)

☐ Kann Nutzer direkt auf diese Daten zugreifen (access by design)? (Art. 3 Abs. 1 Data Act)

- unverzüglich,
- einfach, sicher,
- unentgeltlich,
- in einem umfassenden, gängigen und maschinenlesbaren Format
- und – falls relevant und technisch durchführbar – direkt zugänglich

☐ Falls nein, kann Nutzer ohne Weiteres verfügbare Daten einschließlich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten (Art. 3 Abs. 1 Data Act)

- 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 (Art. 4 Abs. 1 Data Act)

☐ Zugang zu sowie die Nutzung oder die erneute Weitergabe von Daten vertraglich beschränkbar (Sicherheitsanforderungen, schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen) (Art. 4 Abs. 2)

☐ Schnittstelle erlaubt Wahlfreiheit (Art. 4 Abs. 4 Data Act)

3. Datenbereitstellung an Dritte

☐ Kann der Nutzer verlangen, dass Daten an Dritte weitergegeben werden, kein Torwächter? (Art. 5 Data Act)

☐ Gibt es technische Schnittstellen (API)? (Art. 5 Abs. 2 Data Act)

☐ FRAND – Klauseln für Bereitstellung (Art. 8,9 Data Act)

4. Transparenzpflichten

☐ Werden Nutzer vor Vertragsschluss informiert? (Art. 3 Abs. 2 Data Act)

- Art, Format, Umfang Daten, kontinuierliche Echtzeitgenerierung,
- Speicherort, Speicherdauer
- Modalitäten Zugriff, Abruf, Löschung, Nutzungsbedingungen, Dienstqualität

5. Vertragsgestaltung

☐ Entsprechen Bedingungen dem FRAND-Standard? (Art. 13 Data Act)

6. Schutz von Geschäftsgeheimnissen

☐ Maßnahmen zum Schutz, z.B. Klauseln (Art. 4 Abs. 6.; 5 Abs. 9 Data Act)

☐ Mechanismen falls keine Einigung? (Art. 4 Abs. 7,8M art. 5 9, 10 Data Act)

7. Sicherheit & Datenschutz

☐ DSGVO wird eingehalten? (Art. 1 Abs. 5 Data Act)

* Nicht abschließend

Checkliste: Ist mein Produkt schon “Data Act“ ready?

5.1 Applicability of trade secret arrangements

- 5.1.1 The protective measures agreed on in clauses 5.2. and 5.3 of this Contract, as well as the related rights agreed in clause 5.4, apply exclusively to Data or metadata included in the Data to be made available by the Data Holder to the User, which are protected as trade secrets (as defined in the Trade Secrets Directive, held by the Data Holder or another Trade Secret Holder (as defined in that Directive).
- 5.1.2 The Data identification of data protected as trade secrets and the identity of the Trade Secret Holder(s) are set out in Appendix 4.

The Data Holder declares to the User that they have all relevant rights from any third-party trade secrets holder to enter into this Contract regarding the Data protected as trade secrets.

In accordance with Article 4(6) of the Data Act, ‘, the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata’.

Therefore, the Data Holder should identify the Data protected as trade secrets in **Appendix 4**. However, the Data Holder should not be obliged to describe the trade secret itself. It is sufficient to identify the Data which must be protected to ensure the confidentiality of the trade secret, if the analysis of such Data could reveal the trade secret.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Markus Fuderer
Rechtsanwalt, www.meisterernst.com
Fuderer@meisterernst.com