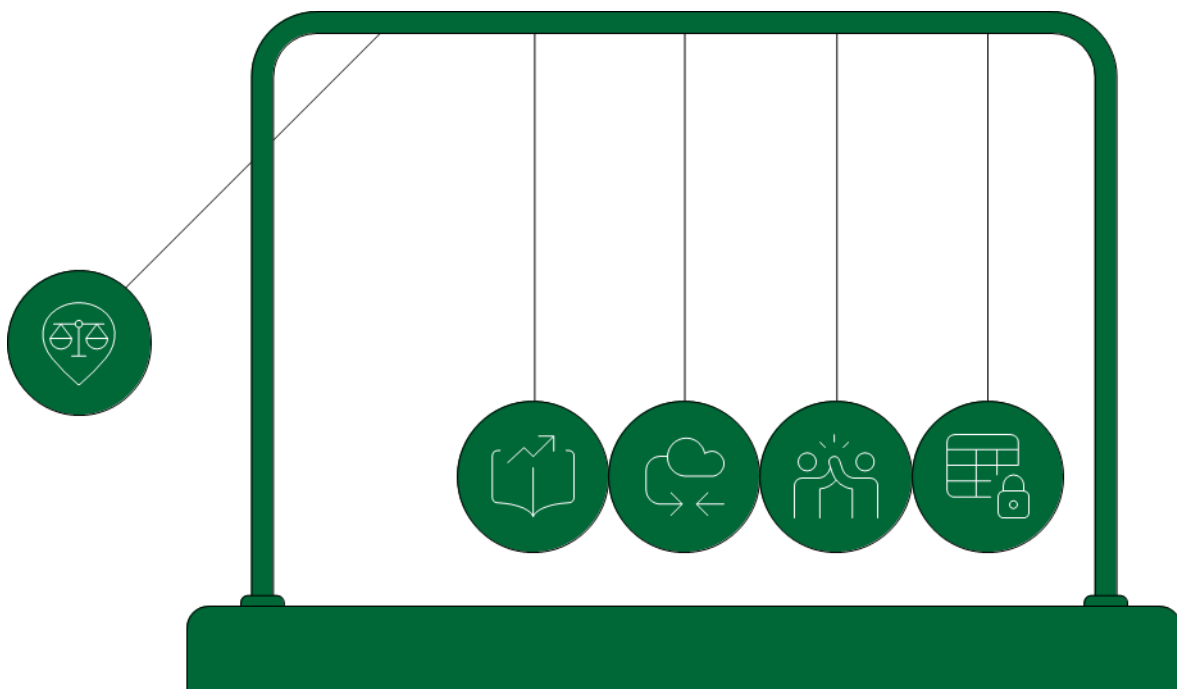


Pflichten für Datenverarbeitungsdienste nach Data Act

Cloud-Switching leicht gemacht?



Einführung

Die Vorschriften der [Verordnung \(EU\) 2023/2854](#), dem sogenannten Data Act (nachfolgend „DA“), gelten seit dem 12.09.2025 unmittelbar in allen EU-Mitgliedstaaten. Die Auswirkungen für die Datenwirtschaft sind dabei weitreichend.

Betroffen von den Vorschriften des DA sind zunächst IoT-Anbieter und solche, die verbundene Dienste anbieten, aber auch sogenannte Datenverarbeitungsdienste. Zu letzteren zählen auch Cloud-Services wie IaaS, PaaS, aber auch SaaS-Dienste. Anbieter solcher Dienste müssen ihren Nutzern umfassende Maßnahmen zur Ermöglichung eines einfachen Anbieterwechsels umsetzen. Der Wechsel, der auch „Cloud-Switching“ genannt wird, verpflichtet Anbieter gleicher Dienstart, Hindernisse zu beseitigen, die einen wirksamen Wechsel ermöglichen. Dazu müssen sie von Gesetzes wegen, bestimmte technische und vertragliche Maßnahmen treffen.

Ziel ist es, den Anbieterwechsel zu erleichtern, damit Abhängigkeiten von Clouddiensten durch einen sogenannten Log-In-Effekt verhindert werden.

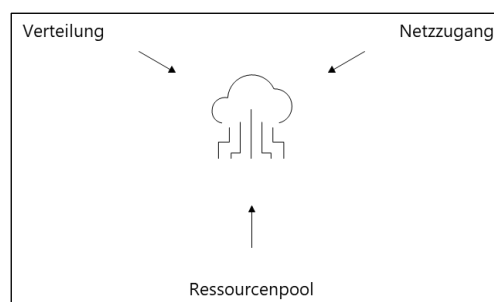
Dieser Leitfaden bietet eine strukturierte Übersicht über die relevanten Pflichten und notwendigen Umsetzungsschritte. Eine Rechtsberatung soll hierdurch jedoch nicht ersetzt werden.

1 Anwendungsbereich: Ist Ihr Unternehmen betroffen?

1.1 Was sind Datenverarbeitungsdienste?

Datenverarbeitungsdienste sind digitale Dienstleistungen, die einen allgegenwärtigen und abrufbaren Netzzugang ermöglichen.¹ Für diese Dienste gelten die Vorschriften des Kapitels 6 DA, das den Wechsel zwischen Datenverarbeitungsdiensten regelt.

Das Gesetz definiert einen „Datenverarbeitungsdienst“ als eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können.²



Datenverarbeitungsdienste = Cloudservices

1.2 Ausnahme: Hochpersonalisierte Dienste

Die Pflichten gelten nicht für sogenannte hochpersonalisierte Dienste. Diese liegen vor, wenn die meisten zentralen Funktionen auf einen einzelnen Kunden zugeschnitten wurden oder alle Komponenten für einen einzelnen Kunden entwickelt wurden. Zusätzlich dürfen diese Dienste nicht im größeren kommerziellen Maßstab über den Dienstleistungskatalog angeboten werden.

1.3 Komplexe Lösungen (Bitkom-Position)

Der Branchenverband BITKOM sieht darüber hinaus auch komplexere Hard- oder Softwarelösungen vom Anwendungsbereich des Kapitels 6 des DA ausgeschlossen.³

Begründet wird dies mit der Anforderung an Datenverarbeitungsdienste, dass diese mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können. Erforderlich sei demnach eine mehr als minimale erstmalige Integration bzw. Implementierungsleistung, also auch eine genauere Abstimmung mit dem Kunden.⁴

Ob sich diese eher restriktive Auslegung durchsetzen wird, ist offen, da sie im Widerspruch zur technologieutralen und weiten Definition von Datenverarbeitungsdiensten in Art. 2 Nr. 8 DA stehen könnte. Es bleibt daher abzuwarten, wie Gerichte dies künftig bewerten werden.

2 Pflichtinformationen für den Kunden

Anbieter von Datenverarbeitungsdiensten müssen ihren Kunden bestimmte Informationen unmittelbar zur Verfügung stellen:

2.1 Auflistung aller Kategorien von Daten, Strukturen und Datenzusammenhängen, die bei einem Wechsel übertragen werden können⁵

Beispiel SaaS-CRM-Dienst:

2.1.1 Datenkategorien

- (1) Kundenstammdaten (Namen, Adressen, Kontaktdaten)
- (2) Kontakthistorie (E-Mails, Anrufe, Meetings)
- (3) Verkaufschancen (Opportunities)
- (4) Angebote und Verträge
- (5) Servicetickets und Support-Anfragen
- (6) Reporting-Daten und Dashboards

2.1.2 Strukturen

- (1) Kundenbeziehungen (Accounts, Contacts, Leads)
- (2) Benutzerdefinierte Felder und Objekte

- (3) Workflow-Definitionen
- (4) Automatisierungsregeln

2.1.3 Datenzusammenhänge

- (1) Verknüpfungen zwischen Kunden und Kontakten
- (2) Zuordnung von Opportunities zu Accounts
- (3) Beziehungen zwischen Tickets und Kunden
- (4) Aktivitätsprotokolle

2.2 Liste der Datenkategorien, die nicht übertragen werden können⁶

Dies gilt für solche Datenkategorien, die untrennbar mit Kundendaten verbunden sind, Geschäftsgeheimnisse enthalten oder bei Übertragung die Sicherheit und Integrität des Kunden oder des Datenverarbeitungsdienstes gefährden würden.

3 Pflichtinformationen für die Öffentlichkeit

Neben den in Ziffer 2 aufgeführten Informationen müssen Anbieter von Datenverarbeitungsdiensten auch die Öffentlichkeit informieren. Auf ihren Webseiten sind bestimmte Informationen bereitzustellen und diese auf dem neuesten Stand zu halten.⁷

3.1 Gerichtsbarkeit

Zu informieren ist über die Gerichtsbarkeit, der die IKT-Infrastruktur unterliegt, die für die Datenverarbeitung der einzelnen Dienste der Anbieter errichtet wurde.

3.2 Allgemeine Beschreibung der technischen, organisatorischen und vertraglichen Maßnahmen

Der Anbieter muss eine allgemeine Beschreibung bereitstellen. Diese beschreibt die technischen, organisatorischen und vertraglichen Maßnahmen zum Schutz nicht-personenbezogener Daten. Die Maßnahmen sollen verhindern, dass staatliche Stellen aus Drittstaaten auf in der EU gespeicherte Daten zugreifen oder diese übermittelt bekommen, wenn dies gegen EU-Recht oder nationales Recht verstoßen würde.



Die Webseiten, auf denen die oben genannten Informationen gepflegt werden, sind dabei in den Verträgen über die Datenverarbeitungsdienste mitaufzuführen.

4 Vertragliche Anforderungen

Die vertraglichen Mindestinhalte ergeben sich aus Art. 25 DA.

4.1 Schriftform

Anbieter von Datenverarbeitungsdiensten müssen die Rechte ihrer Kunden und ihre eigenen Pflichten beim Anbieterwechsel klar in einem schriftlichen Vertrag festlegen.

Der Vertrag muss dem Kunden vor der Unterschrift so bereitgestellt werden, dass er ihn speichern und ausdrucken kann.

4.2 Mindestinhalt

4.2.1 Wechselklausel mit 30-Tage-Frist

Der Kunde hat das Recht, innerhalb von 30 Kalendertagen nach der Kündigung zu wechseln. In dieser Übergangszeit müssen Anbieter:

- (1) **Unterstützung bieten:** d.h. dem Kunden und seinen beauftragten Dienstleistern beim Wechsel helfen..

- (2) **Geschäftsbetrieb aufrechterhalten:** d.h. sorgfältig arbeiten, damit der Service weiterläuft sowie die vertraglich vereinbarten Funktionen weiter bereitstellen.
- (3) **Über Risiken informieren:** d.h. klar über mögliche Unterbrechungen während des Wechsels informieren.
- (4) **Sicherheit gewährleisten:** d.h. hohe Sicherheit während der Datenübertragung sicherstellen und Daten während des gesamten Prozesses schützen.

4.2.2 Unterstützung beim Ausstieg

Der Anbieter hat die Ausstiegsstrategie des Kunden unterstützen, indem er alle relevanten Informationen bereitstellt und den Wechselprozess aktiv begleitet.

4.2.3 Klare Regelung zur Vertragsbeendigung

Der Vertrag endet automatisch, wenn der Wechsel erfolgreich abgeschlossen ist oder die Kündigungsfrist abgelaufen ist und der Kunde seine Daten löschen lassen möchte. Der Kunde muss über die Beendigung informiert werden.

4.2.4 Maximale Kündigungsfrist: 2 Monate

Die Frist, bis der Wechsel beginnen kann, darf höchstens 2 Monate betragen.

4.2.5 Liste aller übertragbaren Daten

Der Anbieter hat vollständig aufzulisten, welche Daten und digitalen Vermögenswerte beim Wechsel übertragen werden können. Dazu gehören mindestens alle exportierbare Daten.

Welche Daten können dies konkret sein?

- (1) Alle Kategorien von Kundendaten
- (2) Alle digitalen Assets (z.B. Konfigurationen, Strukturen)
- (3) Metadaten und Verknüpfungen

4.2.6 Liste der NICHT übertragbaren Daten

Der Anbieter darf bestimmte Daten von der Übertragung ausnehmen, wenn diese für die interne Funktionsweise des Systems spezifisch sind und/oder Geschäftsgeheimnisse enthalten.

Diese Ausnahmen dürfen den Wechsel nicht behindern oder verzögern!

4.2.7 Mindestfrist für Datenabruf: 30 Tage

Nach dem Wechsel muss der Kunde seine Daten noch mindestens 30 Kalendertage lang abrufen können. Diese Frist beginnt nach Ablauf der Übergangszeit.

4.2.8 Löschgarantie

Der Anbieter muss garantieren, dass alle exportierbaren Daten vollständig gelöscht werden und zwar nach Ablauf der 30-Tage-Abruffrist (oder einer längeren vereinbarten Frist). Voraussetzung ist ein erfolgreicher Wechsel.

Welche Daten sind betroffen?

Alle Daten, die direkt vom Kunden erstellt wurden, oder sich direkt auf den Kunden beziehen.

4.2.9 Transparente Gebühreninformation

Der Anbieter muss klar angeben, welche Wechselgebühren erhoben werden (soweit nach Art. 29 DA noch erlaubt).

Wechselentgelte werden schrittweise abgeschafft!

4.3 Was muss der Kunde mitteilen können?

Der Vertrag muss dem Kunden ermöglichen, nach der Kündigung eine der folgenden Optionen zu wählen:

4.3.1 Option A: Wechsel zu einem anderen Anbieter

Der Kunde nennt den neuen Anbieter.

4.3.2 Option B: Wechsel zur eigenen IT-Infrastruktur

Der Kunde übernimmt die Daten selbst.

4.3.3 Option C: Löschung der Daten

Der Kunde möchte die Daten einfach löschen lassen.

4.4 Ausnahme: Längere Übergangszeit bei technischen Problemen

Normalfall: 30 Tage Übergangszeit

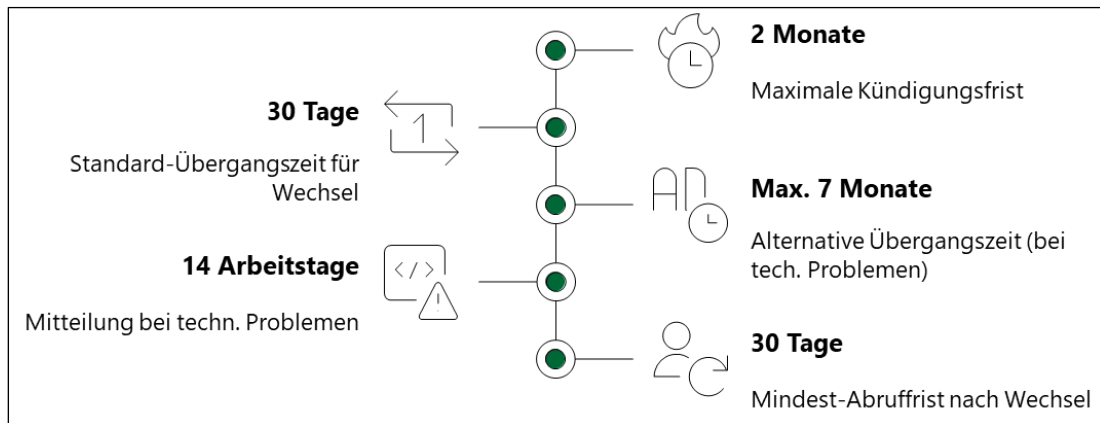
Wenn 30 Tage technisch nicht machbar sind:

- (1) Die Kunde ist innerhalb von 14 Arbeitstagen nach dem Wechselantrag entsprechend zu informieren.
- (2) Der Anbieter muss begründen, warum es technisch nicht möglich ist.
- (3) Der Anbieter muss eine alternative Frist vorschlagen (maximal 7 Monate).
- (4) Während dieser verlängerten Zeit muss der ursprüngliche Service weiter bereitgestellt werden.

4.5 Recht auf Verlängerung durch den Kunden

Der Kunde darf die Übergangszeit einmal verlängern, wenn er mehr Zeit benötigt. Die Dauer der Verlängerung bestimmt der Kunde selbst (im angemessenen Rahmen).

4.6 Die Fristen im Überblick



5 Kündigungrecht und Laufzeitmodelle

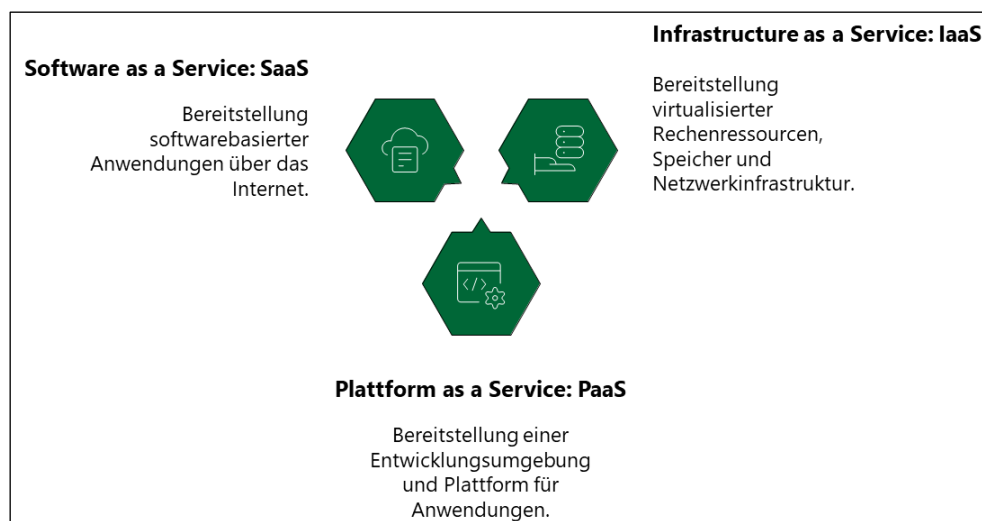
Der DA verbietet dabei weder die Bezahlung externer Dienstleister für Unterstützung beim Anbieterwechsel noch den Abschluss von Verträgen mit fester Laufzeit. Auch verhältnismäßige Vertragsstrafen bei vorzeitiger Kündigung bleiben zulässig, sofern sie mit dem geltenden Recht vereinbar sind.⁸

6 Technische Anforderungen

Der Data Act unterscheidet hinsichtlich der technischen Anforderungen zwischen verschiedenen Arten von Datenverarbeitungsdiensten (Art. 24 Data Act).

Diese Differenzierung ist entscheidend für die Umsetzung der technischen Verpflichtungen beim Anbieterwechsel.

Unterscheidung der Cloud-Dienste



6.1 Offene Schnittstellen

6.1.1 Anforderungen für IaaS-Anbieter

IaaS-Anbieter müssen alle angemessenen Maßnahmen ergreifen, um sicherzustellen, dass der Kunde beim Wechsel zu einem anderen Anbieter oder zu einer eigenen IT-Infrastruktur funktionale Gleichwertigkeit erreichen kann⁹:

- (1) Bereitstellung angemessener Informationen: Umfassende technische Dokumentation über die Infrastruktur, Konfigurationen und Abhängigkeiten
- (2) Technische Dokumentation: Detaillierte Beschreibungen der verwendeten Technologien, Schnittstellen und Systemarchitekturen
- (3) Technische Unterstützung: Aktive Unterstützung während des Wechselprozesses durch qualifiziertes Personal
- (4) Bereitstellung von Kapazitäten und Instrumenten: Zur Verfügungstellung der erforderlichen technischen Werkzeuge und Ressourcen, die für einen reibungslosen Übergang notwendig sind

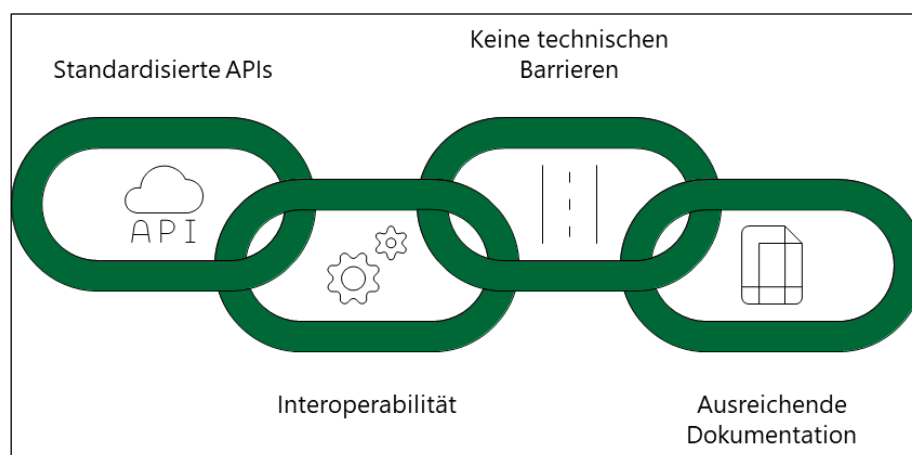
Der IaaS-Anbieter ist nicht verpflichtet, Handlungen in der fremden Infrastruktur des neuen Anbieters vorzunehmen. Die Unterstützung beschränkt sich auf die eigene Infrastruktur und die Bereitstellung aller notwendigen Informationen.

6.1.2 Anforderungen für PaaS- und SaaS-Anbieter

Für Anbieter von Platform-as-a-Service und Software-as-a-Service gelten im Vergleich zu IaaS geringere Anforderungen.¹⁰

Bereitstellung offener Schnittstellen

Um einen reibungslosen Anbieterwechsel zu ermöglichen, müssen PaaS- und SaaS-Anbieter offene Schnittstellen bereitstellen. Diese müssen sowohl dem Kunden als auch dem neuen Anbieter unentgeltlich zur Verfügung gestellt werden.



Kernanforderungen

- (1) **Standardisierte APIs:** Die Schnittstellen müssen den Datenaustausch zwischen verschiedenen Systemen ermöglichen und auf offenen Standards basieren.
- (2) **Interoperabilität:** Die Schnittstellen müssen so gestaltet sein, dass sie die Interoperabilität mit anderen Diensten gewährleisten.
- (3) **Keine technischen Barrieren:** Die Schnittstellen dürfen keine technischen Hindernisse für den Datentransfer schaffen. Export und Import von Daten müssen technisch reibungslos möglich sein, ohne dass proprietäre oder absichtlich komplizierte Mechanismen den Wechselprozess erschweren.
- (4) **Ausreichende Dokumentation:** Die Schnittstellen müssen mit ausreichender Dokumentation versehen sein, sodass interoperable Software entwickelt werden kann.

Anders als bei IaaS-Diensten besteht bei PaaS und SaaS keine Verpflichtung zur Gewährleistung funktionaler Gleichwertigkeit. Die Anforderungen beschränken sich auf die Bereitstellung offener, dokumentierter Schnittstellen für den Datenexport und -import.

6.2 Die Datenformate

Neben den offenen Schnittstellen müssen Anbieter ihre Daten in strukturierten, gängigen und maschinenlesbaren Formaten bereitstellen.¹¹ Hierdurch soll sichergestellt werden, dass die exportierten Daten vom neuen Anbieter oder von der eigenen IT-Infrastruktur des Kunden verarbeitet werden können.

Der DA sieht dabei eine klare Prioritätenordnung für die Wahl der Datenformate und Schnittstellen vor:

6.2.1 EU-Interoperabilitätsspezifikationen

Anbieter von Datenverarbeitungsdiensten müssen vorrangig mit EU-Interoperabilitätsspezifikationen kompatibel sein, sofern solche für ihren Diensttyp verfügbar sind.¹² Die Europäische Kommission wird eine zentrale Unions-Standards-Datenbank ("Central Union Standards Repository") einrichten, in der Bezugnahmen auf harmonisierte Normen und gemeinsame Spezifikationen für die Interoperabilität von Datenverarbeitungsdiensten veröffentlicht werden.¹³ Diese Datenbank dient künftig als verbindliche Referenz für Anbieter von Datenverarbeitungsdiensten.

Für die Übergangsfrist müssen Anbieter die Kompatibilität mit den veröffentlichten Standards mindestens 12 Monate nach deren Veröffentlichung im zentralen Repository gewährleisten.

6.2.2 Strukturierte, gängige und maschinenlesbare Formate

Sind keine EU-Interoperabilitätsspezifikationen für den jeweiligen Diensttyp verfügbar, müssen Daten mindestens in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden (Art. 30 Abs. 5 Data Act).

Zu empfehlen sind standardisierte Datenformate wie z.B. JSON, XML oder CSV.

6.3 Schnittstelleninformationen

Die Bereitstellung offener Schnittstellen allein reicht nicht aus. Anbieter müssen zusätzlich detaillierte Informationen über diese Schnittstellen veröffentlichen. Diese Transparenzpflicht ermöglicht es Kunden und anderen Anbietern, den Wechselprozess zu planen und technisch vorzubereiten.

Zur Erfüllung dieser Pflicht muss eine umfassende technische Dokumentation erstellt werden, die alle relevanten Informationen über die verfügbaren Schnittstellen enthält. Diese Dokumentation sollte Angaben zu den API-Endpunkten, Authentifizierungsmethoden, unterstützten Datenformaten, Übertragungsprotokollen und eventuellen Beschränkungen enthalten. Die Schnittstelleninformationen müssen auf der Webseite des Anbieters veröffentlicht und für Kunden leicht zugänglich gemacht werden. Da sich technische Systeme weiterentwickeln, ist es erforderlich, diese Dokumentation bei Änderungen an den Schnittstellen regelmäßig zu aktualisieren, damit die Informationen stets dem aktuellen Stand entsprechen.

7 Musterklauseln

Die Europäische Kommission hat unverbindliche Musterklauseln entwickelt, um Unternehmen bei der Umsetzung der Data Act-Anforderungen zu unterstützen.¹⁴

Dabei sind zwei Arten von Musterklauseln vorgesehen, nämlich die Model Contractual Terms (MCTs) für Datenzugang und -nutzung und die Standard Contractual Clauses (SCCs) für Cloud-Computing-Verträge. Letztere sind für die Konstellation im vorliegenden Kontext relevant.

Die Musterklauseln bieten keinen fertigen Lösungsansatz. Sie sind unverbindlich und sollten ohne eine Anpassung auf den jeweiligen Fall nicht unmittelbar übernommen werden.

8 Umsetzungsbeispiele der Informationspflichten gemäß Ziffer 2 und 3

Bitte beachten Sie, dass es sich nachfolgend nur um unverbindliche Beispiele handelt. Maßgeblich für die Umsetzung ist der jeweilige Einzelfall.

8.1 Beispiel: Darstellungsmöglichkeit der Pflichtinformationen für Kunden – CRM-Dienst

Empfohlenes Format: Strukturiertes Online-Register

Erstellen Sie ein dynamisches, aktuelles Online-Register, das nachfolgend aufgelistete Elemente enthält. Da es nur den Kunden zur Verfügung gestellt werden muss, kann dies über eine nicht indizierte Webseite erfolgen. Sie müssen dann aber den jeweiligen Link dem Kunden zur Verfügung stellen:

Information gemäß Art. 26 Data Act (DA)

Exportierbare Daten - [Name des Angebots]
 Letzte Aktualisierung: [Datum]

1. Datenkategorien

- Kundenstammdaten (Namen, Adressen, Kontaktdaten)
- Kontakthistorie (E-Mails, Anrufe, Meetings)
- Verkaufschancen (Opportunities)
- Angebote und Verträge
- Servicetickets und Support-Anfragen
- Reporting-Daten und Dashboards

2. Strukturen

- Kundenbeziehungen (Accounts, Contacts, Leads)
- Benutzerdefinierte Felder und Objekte
- Workflow-Definitionen
- Automatisierungsregeln

3. Datenzusammenhänge

- Verknüpfungen zwischen Kunden und Kontakten
- Zuordnung von Opportunities zu Accounts
- Beziehungen zwischen Tickets und Kunden
- Aktivitätsprotokolle

4. Verfügbare Wechselverfahren und -methoden

Exportmethoden:

- API-basierter Export über REST-Schnittstelle
- Manueller Download über Kundenportal
- Automatisierter Export auf Anfrage

Verfügbare Datenformate:

- JSON (Standard nach ISO/IEC 21778)
- CSV (UTF-8, Trennzeichen: Semikolon)
- XML (nach ISO 20022)

Technische Einschränkungen:

- Maximale Dateigröße pro Export: 5 GB
- API-Ratenlimit: 1.000 Anfragen pro Stunde
- Bandbreitenbegrenzung: 100 Mbit/s

Bekannte Beschränkungen:

- Verschlüsselte Anhänge müssen separat exportiert werden
- Echtzeitdaten haben eine Verzögerung von max. 15 Minuten

5. Folgende Daten können NICHT übertragen werden:

- Proprietäre KI-Algorithmen
Grund: Geschäftsgeheimnis gemäß Art. 24 Abs. 3 lit. b) DA
- Aggregierte Benchmarking-Daten
Grund: Gefährdung der Sicherheit anderer Kunden gemäß Art. 24 Abs. 3 lit. c) DA
- Interne Systemlogs mit Sicherheitsinformationen
Grund: Gefährdung der Systemintegrität gemäß Art. 24 Abs. 3 lit. c) DA

8.2 Beispiel: Darstellungsmöglichkeit der Pflichtinformationen für die Öffentlichkeit

Erstellen Sie eine dedizierte Webseite (z.B. /data-act-compliance oder /switching-information). Auf dieser Webseite sind dann die folgenden Informationen darzustellen:

Informationen gemäß Art. 28 Data Act (DA)

1. Datenverarbeitungsorte und Gerichtsbarkeit

Service: [Name des Angebots]

- a) Primärer Standort: Frankfurt/Main, Deutschland; Gerichtsbarkeit: Deutschland / EU
- b) Backup-Standort: Amsterdam, Niederlande; Gerichtsbarkeit: Niederlande / EU
- c) Content Delivery Network (CDN)-Knoten: EU-weit; Gerichtsbarkeit: Jeweiliger EU-Mitgliedsstaat

2. Schutz vor Drittstaaten-Zugriff

Allgemeine Beschreibung der Schutzmaßnahmen

a) Technische Maßnahmen

- Ende-zu-Ende-Verschlüsselung (AES-256-GCM)
- Geografisches Access Management mit EU-Lokalisierung
- Automatische Anomalieerkennung bei Zugriffsversuchen
- Data-at-Rest-Verschlüsselung auf allen Speichersystemen

- Netzwerksegmentierung nach EU-Standorten

b) Organisatorische Maßnahmen

- Richtlinie zur Ablehnung unrechtmäßiger Datenanfragen aus Drittstaaten
- Mehrstufiges Eskalationsverfahren an Rechtsabteilung und Datenschutzbeauftragten
- Verpflichtung aller Mitarbeiter auf EU-Datenschutz- und Datensicherheitsstandards
- Regelmäßige Compliance-Audits (vierteljährlich)
- Dokumentation aller Zugriffersuche staatlicher Stellen
- Schulungsprogramm für Mitarbeiter zu Data Act und internationalen Datentransfers

c) Vertragliche Maßnahmen

- Verpflichtung von Subdienstleistern auf EU-Standards durch vertragliche Vereinbarungen
- Verbot der Datenweitergabe ohne EU-Rechtsgrundlage
- Kündigungsrechte bei Rechtsänderungen in Drittstaaten, die Datenzugriffe ermöglichen würden
- Transparenzpflichten gegenüber Kunden bei staatlichen Zugriffersuchen
- Durchsetzbare Vertragsstrafen bei Verstößen gegen Datenlokalisierungspflichten

Vollständige technische Dokumentation und detaillierte TOMs:
[[Link zu den detaillierten TOMs](#)]

Kontakt: [E-Mail-Adresse]

Referenzieren Sie in Ihren Verträgen auf die Webseiten mit den entsprechenden Informationen.

Beispiel:

„Informationen über Gerichtsbarkeit und Schutzmaßnahmen gemäß Art. 26 und Art. 28 Data Act finden Sie auf unseren Compliance-Webseiten: [www.beispiel.de/data-act-compl...] ...]

Diese Informationen werden regelmäßig aktualisiert. Der Anbieter informiert den Kunden über wesentliche Änderungen per E-Mail an die im Vertrag hinterlegte Kontaktadresse.“

8.3 FAQ-Sektion zum Anbieterwechsel

Eine weitere Möglichkeit könnte darin bestehen, eine FAQ-Seite zum Anbieterwechsel zu erstellen. Diese könnte folgenden Inhalt haben:

Häufig gestellte Fragen zum Anbieterwechsel

Gemäß Data Act (Kapitel VI) haben Sie als Kunde eines Datenverarbeitungsdienstes folgende Rechte beim Anbieterwechsel:

Wie lange dauert ein vollständiger Datentransfer?

- Standardfall (Szenario A): Maximal 30 Kalendertage nach Vertragsende
- Bei hoher technischer Komplexität (Szenario B): Bis zu 7 Monate nach begründeter technischer Mitteilung
- Kundeninitiierte Verlängerung: Sie können die Frist jederzeit für Ihre eigenen Zwecke verlängern

In welchen Formaten werden Daten bereitgestellt?

Siehe unser aktuelles Online-Register: [\[Link zum Datenregister\]](#)

Verfügbare Formate:

- JSON (ISO/IEC 21778)
- CSV (UTF-8)
- XML (ISO 20022)

Fallen Kosten für den Wechsel an?

- Bis 12.01.2027: [\[Link zur Kostenübersicht Wechselentgelte\]](#)
- ab 12.01.2027: Vollständig kostenlos gemäß Art. 29 Data Act

Welche Unterstützung erhalte ich beim Wechsel?

- Technische Dokumentation und API-Zugang
- Persönlicher Support während der Übergangsphase
- Bereitstellung offener Schnittstellen für PaaS/SaaS-Dienste
- Sicherstellung der Datenverfügbarkeit während des Wechsels

Wie kündige ich meinen Vertrag für einen Wechsel?

- Maximale Kündigungsfrist: 2 Monate gemäß Art. 25 Abs. 2 lit. d) Data Act
- Kündigung per E-Mail an: [\[E-Mail-Adresse\]](#)

Nach der Kündigungsfrist beginnt automatisch die Übergangsphase.

Was passiert mit meinen Daten nach dem Wechsel?

- Daten bleiben mindestens 30 Kalendertage nach Wechselabschluss abrufbar
- Anschließende Löschung, sofern keine gesetzliche Aufbewahrungspflicht besteht
- Löschbestätigung auf erfolgt auf Anfrage

© [2026] [VARY.LEGAL GmbH]. Dieses Werk ist lizenziert unter einer Creative Commons

Namensnennung - Nicht-kommerziell - Keine Bearbeitungen 4.0 International Lizenz.

Um eine Kopie dieser Lizenz zu sehen, besuchen Sie <http://creativecommons.org/licenses/by-nc-nd/4>

Disclaimer

Dieses Whitepaper dient ausschließlich Informationszwecken und stellt keine Rechts-, Steuer-, Anlage- oder sonstige Beratung dar. Die Informationen werden ohne Gewähr für Vollständigkeit, Richtigkeit oder Aktualität bereitgestellt. Die Nutzung der Informationen in diesem Dokument erfolgt auf eigenes Risiko. Es wird empfohlen, vor Entscheidungen fachkundigen Rat einzuholen.

VARY.LEGAL GmbH ist spezialisiert auf rechtliche Fragestellungen im Bereich der digitalen Datenwirtschaft. Das Team berät Unternehmen bei der Umsetzung europäischer Datenvorschriften und unterstützt insbesondere bei der rechtssicheren Implementierung der Anforderungen des Data Act für Cloud-Service-Provider.

¹ Art. 2 Nr. 8 DA

² Art. 2 Nr. 8 DA

³ <https://www.bitkom.org/sites/main/files/2025-09/bitkom-leitfaden-umsetzung-data-act.pdf>

⁴ Art. 2 Nr. 8 DA

⁵ Art. 25 Abs. 2 lit. e DA

⁶ Art 25 Abs. 2 lit. f DA

⁷ Art. 28 Abs. 1 DA

⁸ ErwG 89 DA

⁹ Art. 30 I DA

¹⁰ Art. 30 II DA

¹¹ Art. 30 V DA

¹² Art. 31 DA

¹³ Art. 35 Abs. 8 DA, die Datenbank existiert aktuell noch nicht, siehe auch: <https://digital-strategy.ec.europa.eu/en/policies/data-act>

¹⁴ Art. 41 DA, die Musterklauseln stehen unter: <https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding> zur Verfügung