in bestimmten Teilbereichen auch

- der Digital Markets und der
- AI Act.

4. Für welche Unternehmen ist das Datenrecht relevant?

Das Datenrecht ist nicht nur für bestimmte Unternehmen relevant. Es kann wird erwartungsgemäß sowohl für große als auch kleine Unternehmen, etablierte Player und Start-ups einschlägig sein. Es ist auch keineswegs so, dass ausschließlich im Digitalbereich führende Unternehmen von diesen Regelungen betroffen sein könnten. Es ist zu erwarten, dass das Datenrecht für eine Vielzahl an Marktteilnehmern eine beutende Rolle einnimmt. Auch eine Einschränkung auf eine bestimmte Branche gibt es nicht.

5. Haben Unternehmen davon auszugehen, dass ihnen das Datenrecht nur zusätzliche Compliance-Aufgaben auferlegt, oder können sie davon auch profitieren?

Die Antwort auf diese Frage hängt vom Einzelfall ab. Dass es zu einem erhöhten Compliance-Aufwand kommen kann, ist ein Faktum. Dennoch besteht – je nach Ausgangslage – auch das Potenzial, dass Unternehmen von datenrechtlichen Bestimmungen profitieren. Zu denken ist in diesem Zusammenhang insbesondere an erweiterte Möglichkeiten, Zugang zu Daten zu erlangen. Eine Befassung mit dem Datenrecht lohnt sich daher aus beiden Gesichtspunkten heraus.

6. Gilt das Datenrecht nur für Unternehmen mit Sitz in der EU?

Diese Frage ist grundsätzlich für den jeweiligen „Act" gesondert zu beurteilen. Allen zuvor genannten *Acts* ist aber gemeinsam, dass ihnen das Marktortprinzip zugrunde liegt. Das bedeutet eine Geltung unabhängig vom Ort der Niederlassung der Hersteller oder Anbieter. Es ist ausreichend, dass die betreffenden Produkte in der EU angeboten werden. Am Beispiel des Data Act: in räumlicher Hinsicht erstreckt sich der Anwendungsbereich des Data Act nach Art 1 (3) DA auf IoT-Produkte, die in der EU auf den Markt gebracht werden, unabhängig von der Niederlassung des Herstellers.

7. Führt die EU-Regeln zum Datenrecht, insbesondere der Data Act, das Dateneigentum ein?

Nein. Es wird kein Dateneigentum eingeführt. Der Data Act sieht Zugangsrechte an Daten vor, aber keine ausdrückliche sachenrechtliche Zuordnung an Daten. Zur Eigentumsfrage äußert er sich nicht. Allerdings darf ein Dateninhaber Daten uU nur auf der Grundlage eines Vertrags mit dem Nutzer nutzen,[2] wodurch der

2 Art 4 Z 13 DA.

2. Datenzugang (Art 3 DA) und Datenbereitstellung (Art 4 und 5 DA)

Folgende Fragen werden in diesem Kapitel beantwortet:

- Was ist – begrifflich – der Unterschied zwischen Datenzugang und Datenbereitstellung?
- Wann besteht ein Anspruch auf Datenzugang bzw eine Pflicht, einen solchen einzuräumen?
- Wann besteht ein Anspruch auf Datenbereitstellung bzw eine Pflicht, eine solche vorzunehmen?
- Betrifft dies sämtliche Daten oder nur bestimmte? Welche Daten sind erfasst?

Wichtige Ergebnisse dieses Kapitels kurz zusammengefasst

Der Data Act normiert einen Anspruch auf Datenzugang bzw eine Verpflichtung, einen solchen einzuräumen. Dafür müssen bestimmte Voraussetzungen erfüllt sein. Entscheidend ist zunächst, wodurch die Daten generiert werden. Maßgebliche Anknüpfungspunkte sind vor allem das *vernetzte Produkt* und der *verbundene Dienst*. Letztlich bestimmen noch weitere Faktoren, welche Daten unter die Datenzugangsrechte fallen. Allgemein gesagt fallen Rohdaten und aufbereitete Daten, die für den Dateninhaber infolge der technischen Gestaltung des Produktes bzw Dienstes leicht verfügbar sind, darunter.

Nicht jeder hat einen Anspruch auf Datenzugang, sondern nur der *Nutzer*; dies auch nicht gegenüber jedermann, der Daten hält, sondern nur gegenüber dem *Dateninhaber*. Auf Verlangen des Nutzers können die Daten auch an bestimmte Dritte, die *Datenempfänger*, herauszugeben sein.

Begrifflich wird hier differenziert zwischen Datenzugang und Datenbereitstellung, wobei ein wesentlicher Unterschied darin besteht, dass Datenzugang *direkt*, dh ohne eine gesonderte darauf gerichtete Anfrage des Nutzers, gewährt werden muss, während bei der Datenbereitstellung eine solche Anfrage notwendig und der Zugriff daher nur *indirekt* ist.

Dass die Daten beim Datenzugang sohin direkt über das jeweilige Produkt auslesbar sein sollen, müssen Hersteller bereits bei der Produktgestaltung beachten. Man spricht daher auch von einer Konzeptionierungspflicht.

2.1. Einleitung

Bei den in diesem Kapitel behandelten Bestimmungen handelt es sich um den wohl zentralen Aspekt des DA. Wie in den FAQs beschrieben, ist es ein wesentliches regulatorisches Anliegen, Datensilos aufzubrechen und Daten für mehrere verschiedene Marktteilnehmer verfügbar zu machen. Der DA sieht bestimmte Instrumente vor, um dieses Ziel zu erreichen. Dazu zählen die Regelungen zum Datenzugang bzw zur Datenbereitstellung.

Die grundlegenden Bestimmungen, die in diesem Zusammenhang maßgeblich sind, sind in erster Linie jene des Art 3 Abs 1 DA einerseits und jene des Art 4 Abs 1 und Art 5 Abs 1 DA andererseits. Sie legen die grundsätzliche Funktionsweise des Datenzugangs bzw der Datenbereitstellung fest. Begrifflich wird hier – auch, um die bestehenden materiellen Unterschiede deutlich zu machen – unter-

2.5.1. Datenzugang „by Design" nach Art 3 DA

2.5.1.1. Grundlegendes

Nach Art 3 Abs 1 DA werden vernetzte Produkte so konzipiert und hergestellt und verbundene Dienste so konzipiert und erbracht, dass die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.

Damit wird eine Verpflichtung vorgeschrieben, das vernetzte Produkt bzw den verbundenen Dienst auf eine bestimmte Art zu konzeptionieren. Sie müssen diese Verpflichtung grundsätzlich bereits im Prozess der Produktherstellung bzw der Designphase berücksichtigen. Bereits in diesem Stadium sind die notwendigen technischen Vorkehrungen zu treffen, damit Nutzer ihr Zugangsrecht entsprechend den Vorgaben des DA ausüben können. Deshalb wird regelmäßig auch vom Datenzugang by Design oder einer Konzeptionierungspflicht gesprochen.

Der DA schreibt aber nicht vor, dass bestimmte Daten von einem Produkt generiert werden müssen. Die Entscheidung, ob das geschieht, verbleibt bei den Herstellern. Sie können Produkte und Dienste daher weiterhin so konzipieren, dass bestimmte Daten nicht generiert werden. Entscheiden sie sich aber dafür, ihr Produkt bzw ihren Dienst so zu gestalten, dass bestimmte Daten generiert werden und diese vom Hersteller selbst abgerufen werden können, muss auch der Nutzer Zugang erhalten.[95]

Art 3 Abs 1 DA gilt für vernetzte Produkte und verbundene Dienste, die **nach dem 12.9.2026** in Verkehr gebracht werden.

2.5.1.2. Adressat der Verpflichtung

Adressaten der Konzeptionierungspflicht sind diejenigen, die sie tatsächlich umsetzen können. Bei vernetzten Produkten sind das in erster Linie die Hersteller und bei verbundenen Diensten deren Anbieter.[96]

2.5.1.3. (Technische) Umsetzung des Datenzugangs

Art 3 Abs 1 DA verlangt, dass die Daten dem Nutzer *direkt* zugänglich sein müssen. *Direkt* bedeutet, dass der Nutzer Zugang zu den Daten haben muss, ohne dafür mit einem Zugangsverlangen an den Dateninhaber heranzutreten. Er soll die Daten nicht gesondert anfordern müssen, sondern ohne eine solche Kontaktaufnahme auf sie zugreifen können.[97] Die Zugriffsmöglichkeit hat für ihn eine rein faktische

95 *Denga* in *Specht/Hennemann*, Data Act/Data Governance Act, 2. Auflage 2025, Art 3, Rn 47, 48.
96 *Schreiber/Pommerening/Schoel*, Der neue Data Act, 2. Auflage, S 53, Rz 47.
97 European Commission, FAQs Data Act, Version 1.2., S 13.

mehr werden Daten im DA als Träger von Informationen angesehen.[185] Für den Geschäftsgeheimnisschutz folgt daraus, dass nicht die Daten selbst als Geschäftsgeheimnisse geschützt sein können, sondern die Informationen, die sie beinhalten bzw auf die sie Rückschlüsse ermöglichen.

Eine Information ist **geheim**, wenn sie den relevanten Verkehrskreisen weder allgemein bekannt noch ohne Weiteres zugänglich ist.[186]

Unter **kommerziellem Wert** wird ein aktueller oder potenzieller Handelswert aus Sicht eines objektiven und verständigen Betrachters verstanden.[187] Der Wert muss sich aus der Geheimheit der Information ergeben (kausaler Zusammenhang).[188] Führt eine Offenlegung der Information dazu, dass die Wettbewerbsposition des Informationsinhabers geschwächt wird, indiziert dies einen kommerziellen Wert infolge der Geheimhaltung.

Zuletzt müssen in Bezug auf die Information **angemessene Geheimhaltungsmaßnahmen** ergriffen werden, um Geschäftsgeheimnisschutz für sie beanspruchen zu können. Dies erfordert ein aktives Tätigwerden. Das zum Beispiel in der Form von

i. organisatorischen Maßnahmen, wie Zugangs- und Nutzungsbeschränkungen, Kennzeichnung von Dokumenten als vertraulichen, Mitarbeiterzugang nur auf *Need-to-know*-Basis, Mitarbeiterschulungen;
ii. technischen Maßnahmen, zB durch IT-Security, Verschlüsselung, Passwortschutz;
iii. rechtlichen Maßnahmen, wie insbesondere Geheimhaltungsvereinbarungen mit Vertragspartnern oder Arbeitnehmern.

4.1.3. (Roh-)Daten als Geschäftsgeheimnis

Der Data Act definiert Daten ua als *digitalisierte Informationen*.[189] Auf den ersten Blick scheint das Tatbestandsmerkmal der ***Information*** daher keine Schwierigkeiten zu bereiten. Allerdings gelten die Bestimmungen des Data Act zum Datenzugang bzw zur Datenbereitstellung in erster Linie für Daten in Rohform. Bei diesen hat noch keine Datenanalyse stattgefunden. Die in den Daten gelegenen Informationen sind daher wohl noch nicht bekannt. Deshalb könnten Zweifel daran bestehen, dass Rohdaten überhaupt ein Informationsgehalt zukommt und sie als Geschäftsgeheimnisse in Frage kommen. Allerdings scheiden Rohdaten nicht als Gegenstand des Geschäftsgeheimnisschutzes aus; dies aus mehreren Gründen:

Die Bestimmungen des UWG zum Geschäftsgeheimnisschutz normieren nicht, dass die Information bereits vorliegen muss. Im Umkehrschluss kommen daher

185 *Schippel*, Datenqualität in Data Act und AI Act, KuR 2024, 561.
186 *Thiele* in *Wiebe/Kodek* (Hrsg), UWG § 26b Rz 11.
187 ErwGr 14 Geschäftsgeheimnis-RL, *Görg* in *Görg* (Hrsg), Kommentar zum UWG (2020) § 26b UWG Rz 16.
188 *Hofmarcher*, Das Geschäftsgeheimnis, Rz 2.21.
189 Art 2 Z 1 DA.

Weil, wie noch gezeigt wird, bei Identität zwischen Nutzer und betroffener Person idR vergleichsweise leicht eine datenschutzrechtliche Rechtsgrundlage gefunden werden kann, ist die Bedeutung dieser noch ungeklärten Frage für die Praxis wohl überschaubar.[261]

4.2.4. Mögliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

Die maßgebliche Bestimmung der DSGVO in diesem Zusammenhang ist bei „herkömmlichen" personenbezogenen Daten Art 6 und bei besonderen Kategorien („sensiblen") personenbezogenen Daten Art 9. Dort sind die in Frage kommenden Rechtsgrundlagen, die eine Datenverarbeitung rechtfertigen können, genannt. Welche verwirklicht ist, hängt von den konkreten Umständen und insbesondere auch davon ab, ob der Nutzer gleichzeitig die betroffene Person ist oder nicht. In beiden Szenarien kann es überdies dazu kommen, dass der Nutzer die Datenbereitstellung i) an sich selbst oder ii) einen Dritten fordert.

Es sind somit verschiedene Konstellationen eines Aufeinandertreffens von Datenbereitstellungsverlangen mit der DSGVO denkbar. Welche im Einzelfall verwirklicht ist, entscheidet darüber, was für eine datenschutzrechtliche Rechtsgrundlage (allenfalls) einschlägig ist.

4.2.4.1. Nutzer = betroffene Person

In diesem Szenario verlangt ein Nutzer, der eine natürliche Person ist, die Bereitstellung personenbezogener Daten über die eigene Nutzung des vernetzten Produktes oder verbundenen Dienstes. In seinem Zugangsverlangen wird eine **schlüssige Einwilligung** in diese mit der Zugangseinräumung verbundenen Datenverarbeitung zu sehen sein.[262] Damit liegt für **„herkömmliche" personenbezogene Daten** eine Rechtsgrundlage im Sinne der DSGVO vor.

Bei **besonderen Kategorien personenbezogener Daten**, wie zB und unter dem Data Act relevant die bei der Nutzung eines Fitness-Wearable generierten Gesundheitsdaten, sind die Anforderungen an die Einwilligung allerdings höher. Um als Rechtsgrundlage für die Verarbeitung solcher Daten in Frage zu kommen, muss sie *ausdrücklich* sein, womit die Möglichkeit zur konkludenten Erteilung wegfällt.[263]

261 *Specht-Riemenschneider* in *Specht/Hennemann*, Data Act/Data Governance Act, 2. Auflage 2025, Art 1 Rz 63.

262 *Antoine*, Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht – Achillesferse des Data Act in der Praxis? CR 2024, 73–80; *Wienroeder*, Sind der Data Act und die DSGVO miteinander kompatibel? PinG 2024, 103–108; *Schemmel*, Data Act und DSGVO – ziemlich beste Feinde? CB 2024, 301.

263 *Kastelizu/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm, Art 9 DSGVO Rz 31.

Wenn aber ein Dritter (Datenempfänger) Daten, die Geschäftsgeheimnisse beinhalten, an einen anderen Dritten (zweiten Datenempfänger) weitergibt, und dieser andere Dritte (bzw zweite Datenempfänger) seinen vertraglichen Geheimnisschutzpflichten gegenüber dem ersten Dritten nicht nachkommt, findet auch dadurch ein Eingriff in die Geschäftsgeheimnisse des Dateninhabers (bzw Geschäftsgeheimnisinhabers) statt. Dem Dateninhaber (bzw Geschäftsgeheimnisinhaber) hilft in dieser Konstellation die Verbotsbestimmung des Art 6 Abs 2 lit g DA als Schutzgesetz. Obwohl er in keinem Vertragsverhältnis zum rechtsverletzenden anderen Dritten (zweiten Datenempfänger) steht, kann er gegen diesen vorgehen, ohne dass es darauf ankommt, ob der erste Dritte (Datenempfänger) seiner Pflicht zur Überbindung der Vertraulichkeitsvereinbarung gemäß Art 6 Abs 2 lit c DA nachgekommen ist.[376]

Keine Exklusivität[377]

Dritte dürfen Nutzer, die Verbraucher sind, nicht zu einer exklusiven Datenbereitstellung an den Dritten verpflichten. Auch eine vertragliche Vereinbarung zu diesem Zweck ist unzulässig. Nutzer, die Verbraucher sind, müssen die Möglichkeit haben, die von ihnen bezogenen Daten auch weiteren Dritten bereitzustellen. Daran dürfen sie vom ersten Dritten (Datenempfänger) nicht gehindert werden.

Dieses Verbot kommt nicht nur dem Nutzer, der Verbraucher ist, zugute, sondern indirekt auch potenziellen weiteren Datenempfängern und damit – in der Theorie – Datenmärkten an sich. Die Einschränkung auf Verbraucher bedeutet aber dennoch, dass eine solche Exklusivitätsvereinbarung unter Unternehmen zulässig ist.

5.3.2.3. Vorgaben für das Verhältnis Dateninhaber – Dritter (Datenempfänger)

5.3.2.3.1. Vertragsgestaltung: FRAND-Bedingungen (Art 8 DA)

a. Grundlegendes

Verlangt der Nutzer vom Dateninhaber eine Datenbereitstellung an einen Datenempfänger, haben der Dateninhaber und der Datenempfänger über diesen Datentransfer einen Datenlizenzvertrag abzuschließen. Darin sind die Modalitäten der Datenbereitstellung zu vereinbaren. Dafür stellt der Data Act in Art 8 einige Vorgaben auf. Diese sind **zwingend**.[378] Die Vereinbarung darf davon nicht zum Nachteil einer Partei – also Dateninhaber und Datenempfänger – oder des Nutzers abweichen.

Die Vorgaben des Art 8 DA sind aber nicht bei sämtlichen Datentransaktionen beachtlich, sondern **nur dann, wenn der Dateninhaber aufgrund des Verlangens**

376 *Sattler* in *Specht/Hennemann*, Data Act/Data Governance Act, 2. Auflage 2025, Art 6 Rz 40.
377 Art 6 Abs 2 lit h DA.
378 Art 12 Abs 2 DA.

6.2. Smart Contracts im Data Act

Unabhängig vom Data Act sind im Wesentlichen zwei verschiedene Einsatzbereiche von Smart Contracts verbreitet; jener der Vertragsdurchführung, bei dem der Smart Contract die Umsetzung bzw Durchsetzung einer getroffenen Vereinbarung sicherstellt und jener des Vertragsabschlusses selbst, wobei etwa autonom handelnde Softwareagenten die Verhandlung und den Abschluss des Vertrags *(Machine-to-Machine – M2M)* übernehmen.[448] Der Data Act fokussiert seinem Wortlaut nach rein auf den ersten Typus der **Vertragsdurchführung**.

Dementsprechend definiert der Data Act den Smart Contract – *den intelligenten Vertrag* – als ein

> Computerprogramm, das für die automatisierte Ausführung einer Vereinbarung oder eines Teils davon verwendet wird, wobei eine Abfolge elektronischer Datensätze verwendet wird und die Integrität dieser Datensätze sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet werden.[449]

Dieser Begriff des Smart Contract bezeichnet daher keinen Vertrag im rechtlichen Sinn, sondern einen Programmcode.[450] Im Programmcode werden Bedingungen festgelegt, bei deren Eintritt bzw Nicht-Eintritt automatisch eine bestimmte, vordefinierte Aktion gesetzt wird (*Wenn-dann-Bedingung*). Diese Aktion kann zB die Bereitstellung der Daten oder auch der Entzug des Zugriffs darauf im Falle eines Verstoßes sein. Für die Abwicklung von Datentransaktionen durch Smart Contracts wäre demnach keine menschliche Intervention erforderlich, weil das Computerprogramm selbstständig prüft, ob eine Vertragsklausel erfüllt wurde und ausgehend von diesem Prüfungsergebnis eine Ausführungshandlung vornimmt (bzw unterlässt).

Regelmäßig bauen Smart Contracts auf der Blockchain-Technologie auf, um die automatische Transaktionsabwicklung unabhängig von einer dritten, vertrauenswürdigen Stelle ausführen zu können. Notwendig ist das aber nicht, um als Smart Contract iSd DA zu gelten. Der DA ist diesbezüglich technologieneutral.[451]

Das Potenzial von Smart Contracts bei Datentransaktionen

Smart Contracts können sicherstellen bzw absichern, dass

- Daten erst nach Eingang einer Zahlung oder Vornahme einer sonstigen Gegenleistung bereitgestellt werden;
- Zugriff zu Daten nur bestimmten Personen nach erfolgreichem Durchlaufen einer Identitätsprüfung nach Erfüllung definierter Kriterien gewährt wird;

448 *Leyens/Heiss/Soritz*, Smart Contracts im unternehmerischen Rechtsverkehr (B2B), JBl 2022, 137; *Hanzl/Rubey*, The smartest contract? Zak 2018/350.

449 Art 2 Z 39 DA.

450 *Mofidian/Smets,* Smart Contracts im Zivil- und Gesellschaftsrecht, in *Piska/Vökel* (Hrsg), Blockchain rules[2] (2024) S 153 Rz 5.1.

451 ErwGr 104 DA.

7.7.1. Grundlegendes

Soweit die Trainings-, Validierungs- und Testdatensätze einen Personenbezug aufweisen, gilt die DSGVO. Die Datenverarbeitung muss dann den datenschutzrechtlichen Vorgaben entsprechen. Selbst eine Compliance mit dem AI Act ersetzt keine datenschutzrechtliche Prüfung. Es muss daher insbesondere im Sinne der DSGVO eine **Rechtsgrundlage für die Datenverarbeitung** vorhanden sein. Das gilt nicht nur für Datenverarbeitungen **beim Betrieb des KI-Systems**, sondern gleichermaßen für vorgelagerte Verarbeitungsvorgänge, wie die **Datenbeschaffung** und die **Aufbereitung der Daten**, sowie deren Einsatz für das **Training, die Validierung oder das Testen**. Die einzelnen Verarbeitungstätigkeiten müssen voneinander abgegrenzt und, soweit personenbezogene Daten involviert sind, für jede gesondert geprüft werden, ob eine Verarbeitungsgrundlage nach der DSGVO besteht. Dabei muss unterschieden werden, ob „herkömmliche" personenbezogene Daten oder besondere Kategorien – sogenannte „sensible" – personenbezogenen Daten betroffen sind. Bei Letzteren sind die Anforderungen strenger. Es stehen unterschiedliche Rechtsgrundlagen zur Rechtfertigung der Datenverarbeitung zur Verfügung.

Welche Auswirkungen hätte das Training eines KI-Modells ohne Rechtsgrundlage auf die Nutzung des KI-Modells (bzw eines KI-Systems auf dessen Basis)?

1. **Hohe Bußgelder**
   Die DSGVO sieht empfindliche Strafen vor, nämlich bis zu EUR 20 Millionen oder 4 % des weltweiten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr.[518]
2. **Schadensersatzforderungen**
   Betroffene Personen können individuelle Schadensersatzansprüche geltend machen, wenn ihre Rechte verletzt wurden. Sowohl materielle als auch immaterielle Schäden sind ersatzfähig. Bei einer Vielzahl an betroffenen Personen können auch bei einzelnen, betraglich überschaubaren Ansprüchen in Summe hohe Zahlungen notwendig werden.[519]
3. **Abmahnungen, Klagen und Reputationsverlust**
   Unternehmen können von Konkurrenten oder Verbraucherschutzverbänden abgemahnt und insbesondere auf Unterlassung geklagt werden. Bei Bekanntwerden der Datenschutzverletzung droht zudem ein Reputationsverlust.

7.7.2. Rechtsgrundlagen bei „herkömmlichen" personenbezogenen Daten

Sofern keine „sensiblen" personenbezogenen Daten iSd Art 9 DSGVO betroffen sind, können idR die folgenden Rechtsgrundlagen in Betracht gezogen und geprüft werden:

518 Art 83 Abs 5 DSGVO.
519 Art 82 Abs 1 DSGVO.

11.2. Durchsetzung vor den mitgliedstaatlichen Zivilgerichten (private enforcement)

11.2.1. Allgemeines

Der Data Act enthält **keine** Regelungen zur privatrechtlichen Durchsetzung vor den Zivilgerichten der einzelnen Mitgliedstaaten. Das führt zur grundlegenden Frage, ob nach dem Willen des EU-Gesetzgebers überhaupt eine Möglichkeit zu einem solchen *private enforcement* bestehen soll. Dies ist zu bejahen. Der Umstand, dass im Data Act eine ausdrückliche Regelung dazu fehlt, ist nicht dahingehend auszulegen, dass ein solches nicht erwünscht ist bzw nicht möglich sein soll. Vielmehr scheinen einige Bestimmungen im Data Act die privatrechtliche Rechtsdurchsetzung implizit vorauszusetzen.[652]

Außerdem sind gerade die einen wichtigen Grundpfeiler des Data Act darstellenden Bestimmungen zu Datenlizenzverträgen und den inhaltlichen Vorgaben dafür privatrechtlicher Natur, sodass Meinungsverschiedenheiten zwischen den involvierten Akteuren typischerweise vor Zivilgerichten zu klären wären. Wie bereits in anderen Kapiteln gezeigt, bergen die Regelungen des Data Act einiges an Konfliktpotenzial. Die jeweiligen Akteure werden nicht selten unterschiedliche Interessen verfolgen. Dateninhaber wollen tendenziell so wenig Daten wie möglich herausgeben, während Nutzer und Datenempfänger so viele wie möglich erhalten wollen. Auch rund um die genauen Zugangsbedingungen zu Daten, die Reichweite der erlaubten Datennutzung nach Zugangserhalt, einschließlich der Rechte des Dateninhabers aus Art 11 Abs 2 und 3 Data Act, den Geschäftsgeheimnisschutz, die Unwirksamkeit von Vertragsklauseln oder allfällige schadenersatzrechtliche Ansprüche kann es leicht zu konträren Standpunkten kommen. Nicht selten dürfte sich dabei eine Klage auf dem Zivilrechtsweg (gegebenenfalls in Kombination mit einer einstweiligen Verfügung) besser eignen, um die den einzelnen Akteuren eingeräumten Rechte durchzusetzen. Diese Möglichkeit spricht der Data Act, unbeschadet eines Verwaltungsstrafverfahrens vor der Aufsichtsbehörde, selbst an.[653]

Ein weiteres Argument dafür, dass die zivilrechtliche Rechtsdurchsetzung trotz fehlender Regelung möglich sein soll, ist der Effektivitätsgrundsatz. Danach müssen nationale Rechtsbehelfe eine effektive Umsetzung des Unionsrechts ermöglichen und dürfen den Schutz der dem Einzelnen direkt aus dem Unionsrecht erwachsenden Rechte nicht praktisch unmöglich machen oder übermäßig erschweren. Gäbe es die Möglichkeit zur privatrechtlichen Rechtsdurchsetzung

652 Vgl insb Art 13 Abs 1 (spricht von *Haftung und Rechtsbehelfen bei Verletzung oder Beendigung datenbezogener Pflichten*) und Abs 6 (spricht von *Beweislast*) des DA; so auch: *Schwamberger*, Die zivilrechtliche Durchsetzung von DSGVO, DAS, DA-E und MiCAR im Vergleich, InTer 2023, 168; mE auch noch Art 11 Abs 2 und 3 DA.

653 Art 38 Abs 1 DA.

Der DGA ist zwar bereits seit 24.9.2023 in Geltung, die notwendigen österreichischen Ergänzungsbestimmungen sind aber weiterhin ausständig.

13.2. Weiterverwendung von Daten öffentlicher Stellen

13.2.1. Hintergrund

Öffentliche Stellen verfügen oft über Datenbestände, die nicht frei zugänglich sind. In öffentlichen Datenbanken vorhandene Daten, wie vertrauliche Geschäftsdaten, unter die Geheimhaltungspflicht fallende statistische Daten, durch die Rechte Dritter an geistigem Eigentum geschützte Daten, einschließlich Geschäftsgeheimnissen und personenbezogener Daten, werden oft nicht einmal für Forschungszwecke oder innovative Tätigkeiten im öffentlichen Interesse zur Verfügung gestellt.[706] Der DGA möchte entgegensteuern und Voraussetzungen für den Zugang zu diesen Daten und deren Weiterverwendung **auch für nicht-staatliche Zwecke** schaffen. Er will diesbezüglich einen einheitlichen Mindeststandard schaffen. Daten, die von öffentlichen Stellen oder sonstigen Einrichtungen mithilfe öffentlicher Gelder generiert oder erhoben wurden, sollen auch der Gesellschaft zugutekommen.

Eine **Verpflichtung** für öffentliche Stellen, die von ihnen gehaltenen Daten zu teilen, wird aber **nicht** normiert. Sie müssen die Weiterverwendung der Daten nicht erlauben. Der DGA befreit sie auch nicht von allfälligen Geheimhaltungspflichten.[707] Kommt es aber dazu, können die Vorgaben der Art 3 bis 9 DGA maßgeblich sein.[708]

13.2.2. Anwendungsbereich

Der Anwendungsbereich dieser Bestimmungen ist auf bestimmte Kategorien *geschützter Daten*, die von *öffentlichen Stellen* gehalten und zur *Weiterverwendung* bereitgestellt werden, beschränkt.

Als **geschützt** in diesem Sinn gelten

i. vertrauliche Geschäftsdaten, wie zB Betriebsgeheimnisse, Berufsgeheimnisse, Unternehmensgeheimnisse,
ii. statistische Daten, die einer Geheimhaltungspflicht unterliegen,
iii. Daten, an denen Dritte Schutzrechte des geistigen Eigentums haben oder
iv. personenbezogene Daten, die nicht in den Anwendungsbereich der Open-Data-Richtlinie[709] fallen,

sofern sie sich **im Besitz öffentlicher Stellen** befinden.[710]

706 ErwGr 6 DGA; Art 3 Abs 1 DGA.
707 Art 1 Abs 2 DGA.
708 ErwGr 11 DGA; *Schreiber/Pommerening/Schoel*, Der neue Data Act (2. Auflage), S 154, Rz 3.
709 RL (EU) 2019/1024.
710 Art 3 Abs 1 DGA.