iusnet 15. Juli 2024

Der EU Data Act: werden damit die «Datenschatztruhen» geöffnet?

Martina Arioli

1 ABSTRACT

Im aktuellen Hype um den EU AI Act, der am 2. August 2024 in Kraft treten wird, gerieten gewichtige Rechtsakte der EU etwas aus dem Fokus. Einer darunter ist der EU Data Act, der am 11. Januar 2024 in Kraft trat, einen Eckpfeiler der Europäischen Datenstrategie 2020 darstellt und einen Paradigmenwechsel im Hinblick auf den Datenzugang bringt: Mit dem EU Data Act wird den Nutzerinnen neu ein Anspruch auf Herausgabe ihrer Daten, die bei der Nutzung von vernetzten Produkten generiert werden, gegeben, und sie sollen ihren Cloud-Provider einfacher wechseln können. Die Zuordnung von nicht-personenbezogenen Daten zu einer Nutzerin ist ebenso neu wie auch die grundsätzliche Nutzerzentrierung des EU Data Act, was eine unmittelbare Auswirkung darauf haben wird, wie Produkte und Dienstleistungen hergestellt und vermarktet werden.

Der EU Data Act gilt auch für Anbieter in der Schweiz, wenn sie vernetzte Produkte im EWR in Verkehr bringen, verbundene Dienste an Nutzerinnen im EWR anbieten, Dateninhaber sind, die Daten an Empfängerinnen im EWR bereitstellen oder Dienstleistungen zur Datenverarbeitung an Kunden im EWR erbringen (Cloud- und Edge-Dienstleistungen). Angesichts dessen, dass einige Pflichten am 1. September 2025 in Kraft treten werden, tun Schweizer IoT-Anbieter gut daran, sich mit dem EU Data Act auseinanderzusetzen. Ferner gelten bestimmte Vorgaben für Cloud-Switching bereits ab 11. Januar 2024, weshalb die entsprechenden Verträge bereits heute angepasst werden sollten.

2 ZIELE DES EU DATA ACT

Datengetriebene Technologien hatten in den letzten Jahren einen erheblichen Einfluss auf alle Wirtschaftssektoren und haben den Wert von Daten für verschiedene Akteure erhöht. Hochwertige, interoperable Daten können Wettbewerbsfähigkeit, Innovation und nachhaltiges Wirtschaftswachstum fördern. Heute gibt es jedoch noch zahlreiche Hindernisse bei der Datenweitergabe, wie mangelnde Anreize, rechtliche Unsicherheiten und technische Hürden, die die optimale Nutzung von Daten behindern. Besonders kleine und mittlere Unternehmen (KMU) haben oft nicht die Ressourcen, um Daten effektiv zu nutzen, und stehen vor Zugangsbeschränkungen.

Aus diesem Grund zielt der EU Data Act in erster Linie darauf ab, einen verbindlichen harmonisierten Rahmen für den Datenaustausch zwischen verschiedenen Akteuren und in kommerziellen und nichtkommerziellen Datenökosystemen zu verbessern. Der EU Data Act ist als horizontale Regulierung ein wichtiger Bestandteil im Rahmen des EU-Binnenmarkts für Daten: Daten sollen innerhalb der EU und branchenübergreifend zum Vorteil aller weitergegeben werden können indem klare und faire Regeln für den Datenzugang und die Weiterverwendung von Daten geschaffen werden. Nutzerinnen sollen mit Rechten,

Werkzeugen und Kompetenzen ausgestattet werden, damit sie die volle Kontrolle über ihre Daten behalten bzw. erhalten. So sollen die Nutzerinnen vernetzter Produkte, Folgemarkt-Dienste, Nebendienste und sonstige Dienste nutzen können, die auf diesen Daten basieren.

Das Recht der Nutzerinnen zur Weitergabe an Dritte soll das Entstehen liquider, fairer und effizienter Märkte für nicht-personenbezogene Daten auch für kommerzielle Zwecke ermöglichen (vgl. Erw. 26 EU Data Act). Der EU Data Act bezweckt, die Entwicklung neuer, innovativer vernetzter Produkte oder verbundener Dienste zu fördern und Innovationen auf den Folgemärkten voranzutreiben. Ferner soll die Entwicklung völlig neuartiger Dienste unter Nutzung der betreffenden Daten angeregt werden. Gleichzeitig soll mit dem EU Data Act verhindert werden, dass die Anreize für Investitionen in die Art vernetzter Produkte, von denen die Daten erlangt werden, verloren gehen, etwa wenn Daten zur Entwicklung eines konkurrierenden vernetzten Produkts genutzt werden, das insbesondere aufgrund seiner Merkmale, seines Preises und seines Verwendungszwecks von den Nutzern als austauschbar oder ersetzbar betrachtet wird (Erw. 32).

Betreffend Anbieterwechsel bei Cloud-Dienstleistungen wurden Anbieter von Datenverarbeitungsdiensten bereits mit der Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU angehalten, Verhaltensregeln zu entwickeln und wirksam umzusetzen, die zur Erleichterung des Wechsels des Anbieters von Datenverarbeitungsdiensten und der Übertragung von Daten beitragen sollten. Dieser Selbstregulierungsansatz zeitigte kaum Früchte und es mangelt noch heute an offenen Standards und Schnittstellen, die das Cloud-Switching erleichtern. Der EU Data Act setzt hier mit weitreichenden verbindlichen Pflichten für Anbieter von Cloud und Edge-Dienstleistungen an.

Der EU Data Act enthält sodann weitere Bestimmungen, die auf den ersten Blick etwas arbiträr zusammengewürfelt erscheinen, aber ebenfalls den vorgenannten Zielen dienen sollen. Dieser Beitrag fokussiert auf die drei folgenden Bereiche:

- Datenzugangs- und Datenweitergaberechte der Nutzerinnen von vernetzten Produkten (Ziffer 3);
- Datenzugangsrechte der öffentlichen Hand (Ziffer 4);
- Cloud-Switching (Ziffer 5).

Schliesslich wird die Extraterritorialität des EU Data Act behandelt und der Beitrag schliesst mit dem Versuch einer Abgrenzung und einer Würdigung.

3 DATENZUGANG UND DATENWEITERGABE FÜR NUTZERINNEN VON IOT-ANWENDUNGEN

3.1 Rechte von Nutzerinnen

Mit dem EU Data Act soll sichergestellt werden, dass die Nutzerinnen eines vernetzten Produkts oder verbundenen Dienstes zeitnah auf die Daten zugreifen können, die bei der Nutzung dieses vernetzten Produkts oder verbundenen Dienstes generiert werden (Art. 4 EU Data Act), und dass die Nutzerinnen die Daten auch an Dritte ihrer Wahl weitergeben können (Art. 5 EU Data Act). Diese Daten stellen «digitalisierte Nutzerhandlungen und -vorgänge» dar und sollen dementsprechend für die Nutzerinnen zugänglich sein (Erw. 15 EU Data Act). Als «Nutzerin» gilt eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden

oder die verbundenen Dienste in Anspruch nimmt (Art. 2.12 EU Data Act). Die Nutzerin kann also eine Verbraucherin, ein Unternehmen oder eine öffentliche Stelle sein (für letztere siehe Erw. 18 EU Data Act).

Als „Daten" gelten nach dem EU Data Act 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. 2.1 EU Data Act). Der EU Data Act basiert auf der Dichotomie personenbezogene und nicht-personenbezogene Daten. Für erstere verweist der EU Data Act auf die Definition unter Art 4. 1 DSGVO, als letztere gelten alle Daten, die keine personenbezogenen Daten sind (Art. 2.3 und 2.4. EU Data Act).

Ein „vernetztes Produkt" ist gemäss Art. 2.5 EU Data Act ein 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. Der EU Data Act ist anwendbar auf physische Produkte, die Daten sammeln und diese selbständig elektronisch übermitteln, somit primär Internet of Things (IoT) wie bspw. Fahrzeuge, Smart-Home-Produkte (Waschmaschinen, Kaffeemaschinen, Kühlschränke), Medizinprodukte, intelligente Industriemaschinen, landwirtschaftliche Maschinen, Lifestyleprodukte und weitere Konsumgüter. Vom EU Data Act betreffend Datenzugang und Datenweitergabe nach Art. 5 ff. nicht erfasst sind demgegenüber Produkte bzw. zugehörige Dienste, deren vorrangige Funktion das Speichern bzw. Bearbeiten von Daten ist, wie bspw. PCs, Server, Tablets.

Ein „verbundener Dienst" ist gemäss Art. 2.6 EU Data Act ein digitaler Dienst, der zum Zeitpunkt des Kaufs / Miete / Leasings so mit dem vernetzten Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschliessend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen.

Vernetzte Produkte und verbundene Dienste müssen gemäss Art. 3 EU Data Act so konzipiert und hergestellt bzw. erbracht werden, dass die Produktdaten und verbundenen Dienstdaten – einschliesslich der erforderlichen relevanten Metadaten – standardmässig für die Nutzerin einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.

Damit die Nutzerin überhaupt weiss, dass sie Anspruch auf die mit dem vernetzten Produkt oder verbundenen Dienst generierten Daten hat, führt der EU Data Act umfassende Informationspflichten ein: Gemäss Art. 3.2 EU Data Act müssen Hersteller bzw. Verkäufer, Vermieter oder Leasinggeber die Nutzerin vor dem Erwerb / Abschluss des Miet- oder Leasingvertrags informieren über:

a) die Art, das Format und den geschätzten Umfang der Produktdaten, die das vernetzte Produkt generieren kann;
b) die Angabe, ob das vernetzte Produkt in der Lage ist, Daten kontinuierlich und in Echtzeit zu generieren;
c) die Angabe, ob das vernetzte Produkt in der Lage ist, Daten auf einem Gerät oder einem entfernten Server zu speichern, sowie die vorgesehene Speicherungsdauer;

d) die Angabe, wie die Nutzerin auf die Daten zugreifen, sie abrufen oder gegebenenfalls löschen kann.

Gemäss Art. 3.3 EU Data Act haben auch Anbieter von verbundenen Diensten gegenüber der Nutzerin umfassende Informationsrechte und müssen sie vor Abschluss eines Vertrags informieren über:

a) die Art, den geschätzten Umfang und die Häufigkeit der Erhebung der Produktdaten, die der Dateninhaber voraussichtlich erhalten wird, und gegebenenfalls die Modalitäten, nach denen die Nutzerin auf diese Daten zugreifen oder sie abrufen kann, einschliesslich der Modalitäten des künftigen Dateninhabers in Bezug auf die Speicherung und der Dauer der Aufbewahrung von Daten;
b) die Art und den geschätzten Umfang der zu generierenden verbundenen Dienstdaten sowie die Modalitäten, nach denen die Nutzerin auf diese Daten zugreifen oder sie abrufen kann, einschliesslich der Modalitäten des künftigen Dateninhabers in Bezug auf die Speicherung und der Dauer der Aufbewahrung von Daten;
c) die Angabe, ob der Dateninhaber erwartet, ohne Weiteres verfügbare Daten selbst zu verwenden, und die Zwecke, zu denen diese Daten verwendet werden sollen, und ob er beabsichtigt, einem oder mehreren Dritten zu gestatten, die Daten zu mit der Nutzerin vereinbarten Zwecken zu verwenden;
d) die Identität des Dateninhabers inkl. Kontaktdaten;
e) die Kommunikationsmittel, über die der Dateninhaber schnell kontaktiert werden kann;
f) Angaben, wie die Nutzerin ihr Datenweitergaberecht ausüben oder dieses beenden kann.
g) Informationen über das Beschwerderecht der Nutzerin;
h) die Angabe, ob ein Dateninhaber oder Dritter Inhaber von Geschäftsgeheimnissen ist, die in den Daten enthalten sind, die über das vernetzte Produkt zugänglich sind oder die bei der Erbringung eines verbundenen Dienstes generiert werden;
i) die Dauer des Vertrags zwischen der Nutzerin und dem Dateninhaber sowie Beendigungsmöglichkeiten.

Gemäss Art. 5 EU Data Act haben Nutzerinnen einen Anspruch darauf, dass die Daten, die mit dem vernetzten Produkt oder verbundenen Diensten generiert werden, einem Dritten zur Verfügung gestellt werden, indem sie vom Dateninhaber die Weitergabe der Daten an diesen Dritten verlangen können. Als „Dateninhaber" bezeichnet Art. 2.13 EU Data Act eine natürliche oder juristische Person, die berechtigt oder verpflichtet ist, Daten zu nutzen (siehe hierzu auch Art. 4.13 EU Data Act) und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat. Auftragsbearbeiter bzw. öffentliche Stellen sind keine Dateninhaber (Erw. 22 bzw. Erw. 25 EU Data Act).

3.2 Pflichten von Dateninhabern

Art. 4.1 und Art. 5.1 EU Data Act verpflichten Dateninhaber, die Daten den Nutzerinnen bzw. den von den Nutzerinnen bezeichneten Dritten direkt oder auf einfaches Verlangen hin 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 bereitzustellen.

Die Dateninhaber sind bei einem Datenweitergabegesuch einer Nutzerin gestützt auf Art. 5 EU Data Act verpflichtet, mit dem von der Nutzerin bezeichneten Dritten einen Vertrag abzuschliessen, der gemäss Art. 8 EU Data Act die Bereitstellung der Daten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise regelt. Der Vertrag darf keine missbräuchlichen oder diskriminierenden Klauseln enthalten.

Der Dateninhaber ist zudem verpflichtet, mit der Nutzerin vertragliche Regelungen zu vereinbaren, wenn er nicht-personenbezogene Daten, die vernetzte Produkte und verbundene Dienste generieren, selber nutzen will. Allerdings darf der Dateninhaber dabei keine Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden der Nutzerin nehmen oder die Daten auf andere Art einsetzen, die für die Nutzerin schädigend sein könnte. Mit der Datenweitergabe an Dritte darf der Dateninhaber keine anderen kommerziellen oder nichtkommerziellen Zwecke verfolgen als die Erfüllung des Vertrags mit der Nutzerin. Allenfalls muss der Dateninhaber im Vertrag mit dem Dritten ein Weitergabeverbot überbinden (Art. 4.13 und 4.14 EU Data Act).

Bei personenbezogenen Daten, die nicht von der Nutzerin stammen, muss der Dateninhaber sicherstellen, dass für den Datenzugang der Nutzerin sowie für die Datenweitergabe an Dritte die entsprechenden Vorgaben der DSGVO eingehalten werden (Art. 4.12 und 5.7 EU Data Act).

Ferner hat der Dateninhaber technische Schutzmassnahmen gegen die unbefugte Nutzung oder Offenlegung von Daten sicherzustellen (Art. 11 EU Data Act).

3.3 Einschränkungen der Rechte der Nutzerin

Der Datenzugriff wird durch verschiedene Regelungen im Hinblick auf konkurrierende Produkte / konkurrierende Märkte und Geschäftsgeheimnisse eingeschränkt.

Gemäss Art. 4.10 EU Data Act darf die Nutzerin die Daten weder zur Entwicklung eines anderen konkurrenzierenden vernetzten Produkts nutzen noch einem Dritten weitergeben, der konkurrenzierende Produkte entwickelt / herstellt, noch darf die Nutzerin die Daten benutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers oder des Dateninhabers zu erlangen. Diese Bestimmung soll sicherstellen, dass sich der Datenzugang und die Datenweitergabe nicht wettbewerbsschädigend auswirken.

Auch die Weitergabe an Dritte wird eingeschränkt. So dürfen die Daten nicht an Gatekeeper («Torwächter») nach dem Digital Markets Act weitergegeben werden (Art. 5.3 und 6.2.d EU Data Act). Der Dateninhaber hat also vor der Weitergabe zu prüfen, ob ein Dritter von der EU-Kommission als Torwächter bezeichnet wird. Aktuell betrifft dies diverse grosse Tech-Firmen wie etwa Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft. Ferner sieht der EU Data Act keine Zugangsrechte zugunsten der Öffentlichkeit und/oder der Marktteilnehmer bzw. der Wirtschaft im Allgemeinen vor.

Geschäftsgeheimnisse, die in den Daten von vernetzten Produkten enthalten sind, müssen gewahrt und dürfen nur offengelegt werden, wenn vom Dateninhaber und von der Nutzerin vor der Offenlegung alle Massnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Der Inhaber des Geschäftsgeheimnisses (der nicht unbedingt mit dem Dateninhaber identisch sein muss!) vereinbart mit der Nutzerin angemessene technische und

organisatorische Massnahmen, die erforderlich sind, um die Vertraulichkeit der weitergegebenen Daten zu wahren (Art. 4.6 EU Data Act). Wird hierüber keine Einigung erzielt oder werden die Massnahmen nicht umgesetzt oder wird die Vertraulichkeit der Geschäftsgeheimnisse verletzt, kann der Dateninhaber den Datenzugang gestützt auf Art. 4.7 und 4.8 EU Data Act verweigern. Die Hürden könnten hier relativ hoch angesetzt sein, weshalb es zu einer problematischen Gefährdung der Geschäftsgeheimnisse kommen könnte.

Ferner kann der Datenzugang oder die Datenweitergabe vertraglich eingeschränkt werden, wenn der Datenzugang oder die Datenweitergabe die gesetzlichen Sicherheitsanforderungen für das vernetzte Produkt beeinträchtigen (Art. 4.2 EU Data Act).

3.4 Vertragliche Vorgaben

Damit keine vertraglichen Ungleichgewichte entstehen, enthält der EU Data Act zahlreiche Eingriffe in die Vertragsfreiheit von Unternehmen:

Dateninhaber müssen mit Dritten einen Vertrag abschliessen, der die Datenweitergabe zu fairen, angemessenen und nichtdiskriminierenden Bedingungen (FRAND-Bedingungen) und auf transparente Weise regelt (Art. 8 EU Data Act). Auch macht der EU Data Act Vorgaben, ob der Dateninhaber vom Dritten eine Vergütung für die Datenweitergabe verlangen darf (Art. 9 EU Data Act).

Ferner enthält der EU Data Act zwingende detaillierte Bestimmungen darüber, welche Vertragsklauseln im Zusammenhang mit dem Datenzugang und der Datennutzung als missbräuchlich und damit für die schwächere Partei als unverbindlich gelten, damit die Ausnutzung von Ungleichgewichten vermieden werden kann (Art. 13 EU Data Act). Voraussetzung ist allerdings, dass diese Klauseln der Nutzerin oder dem Dritten vom Dateninhaber einseitig auferlegt werden und es sich auf beiden Seiten um Unternehmen handelt; wenn die Nutzerin oder die Dritte eine Verbraucherin ist, dann gilt das allgemeine, gut ausgebaute EU-Verbraucherschutzrecht.

Vertragsklauseln gelten gemäss Art. 13 dann als missbräuchlich, wenn sie zugunsten der Partei, welche sie einseitig auferlegt hat, insbesondere folgende Regelungen enthalten:

- eine grobe Abweichung von der guten Geschäftspraxis darstellen oder gegen das Gebot von Treu und Glauben verstossen;
- den Ausschluss oder die Beschränkung der Haftung für vorsätzliche oder grob fahrlässige Handlungen;
- den Ausschluss der Rechtsbehelfe bei und der Haftung für Vertragsverletzungen;
- das Recht zur Auslegung des Vertrags einseitig verteilen;
- Datenzugangsrechte und Datennutzungsrechte einseitig zulasten der berechtigten Interessen der anderen Vertragspartei verteilen (z.B. im Zusammenhang mit sensiblen Geschäftsdaten / Geschäftsgeheimnissen / geistigem Eigentum);
- Beschränkungen der angemessenen Datennutzung;
- Einschränkungen des Kündigungsrechts für diejenige Partei, der die Klausel einseitig aufgebürdet wurde bzw. zu kurze Kündigungsfrist für die Partei, welche die Klausel einseitig aufbürdet;
- Beschränkung der Herausgabe einer Kopie der Daten nach Vertragsende;

- einseitige Vertragsänderungen mit Auswirkungen auf Preis oder auf Art, Format, Qualität oder Menge der weiterzugebenden Daten.

Vertragsklauseln gelten als einseitig auferlegt, wenn sie von einer Vertragspartei eingebracht werden und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann. Die Vertragspartei, die die Vertragsklausel eingebracht hat, trägt die Beweislast dafür, dass diese Vertragsklausel nicht einseitig auferlegt wurde (Beweislastumkehrung). Die Vertragspartei, die die beanstandete Klausel eingebracht hat, kann sich nicht darauf berufen, dass es sich um eine missbräuchliche Vertragsklausel handelt (Art. 13.6 EU Data Act).

Rechtsfolge der Feststellung der Missbräuchlichkeit ist die Teilunverbindlichkeit des Vertrags: Wenn die missbräuchliche Vertragsklausel von den übrigen Bedingungen des Vertrags getrennt werden kann, so bleiben die übrigen Vertragsklauseln verbindlich (Art. 13.7 EU Data Act).

Schliesslich sieht der EU Data Act den Erlass von Mustervertragsklauseln durch die EU-Kommission vor (Art. 41 EU Data Act).

4 DATENZUGANG FÜR DIE ÖFFENTLICHE HAND

Gemäss Art. 14 EU Data Act darf die öffentliche Hand um Zugang zu Daten ersuchen und diese Daten an Dritte weitergeben, selbst wenn sie nicht Nutzerin ist. Allerdings ist das Datenzugangsrecht der öffentlichen Hand im Vergleich zum Datenzugangsrecht, welches ihr und anderen Nutzerinnen nach Art. 3 ff. EU Data Act zusteht, stark eingeschränkt: Die öffentliche Stelle muss den Nachweis dafür erbringen, dass im Hinblick auf die Erfüllung ihrer rechtlichen Aufgaben im öffentlichen Interesse die aussergewöhnliche Notwendigkeit der Nutzung bestimmter Daten besteht. Dateninhaber sind nur dann verpflichtet, die Daten bereitzustellen, wenn die öffentliche Stelle einen begründeten Antrag stellt, der den Vorgaben nach Art. 14 ff. EU Data Act entspricht.

Der Antrag der öffentlichen Stelle an den Dateninhaber muss Folgendes enthalten:

- Angaben darüber, dass die Daten zur Bewältigung eines öffentlichen Notstands gemäss Art. 2.29 EU Data Act erforderlich sind (wobei hier der eher unklare Wortlaut von Art. 15.1.b. EU Data Act zu beachten ist);
- Informationen darüber, dass die öffentliche Stelle diese Daten nicht rechtzeitig auf alternative Weise beschaffen kann;
- Angabe der gesetzlichen Grundlage für die öffentliche Aufgabe sowie Angabe des Zwecks, für welchen die Daten gebraucht werden;
- Angaben über die verlangten Daten, deren Umfang sowie die Häufigkeit des Zugangs der öffentlichen Stelle;
- den Nachweis der Verhältnismässigkeit;
- die Dauer der Nutzung der Daten (Andauern des öffentlichen Notstands);
- die Löschfrist;
- die Begründung für die Wahl des Dateninhabers, an den der Antrag gerichtet ist;
- die Bezeichnung der öffentlichen Stellen und Outsourcing-Partner, an welche die Daten (sofern notwendig) weitergegeben werden;

- Zusage der Gewährleistung der Wahrung von Geschäftsgeheimnissen;
- Umschreibung der technischen und organisatorischen Massnahmen zum Schutz der personenbezogenen Daten, soweit diese nicht pseudonymisiert (bzw. anonymisiert, vgl. Art. 17.1.g EU Data Act) werden können.

Der Antrag muss schriftlich und in klarer, prägnanter, einfacher und für den Dateninhaber verständlicher Sprache abgefasst sein. Die EU-Kommission wird ein Musterformular erstellen. Der Antrag wird sodann von der zuständigen Behörde veröffentlicht. Der angefragte Dateninhaber kann dem Antrag nur gestützt auf einen der in Art. 18 EU Data Act angeführten Gründe ablehnen. Wenn der Dateninhaber im Falle eines öffentlichen Notstands kein KMU ist, muss er die Daten der öffentlichen Stelle unentgeltlich zur Verfügung stellen (Art. 20.1 EU Data Act).

Die öffentliche Stelle darf sodann die Daten nicht zur Erlangung von Kenntnissen über die wirtschaftliche Lage, die Vermögenswerte und Produktions- oder Betriebsmethoden des Dateninhabers nutzen, um ein vernetztes Produkt oder einen verbundenen Dienst zu entwickeln oder zu verbessern, das bzw. die mit dem vernetzten Produkt oder dem verbundenen Dienst des Dateninhabers im Wettbewerb steht oder einem Dritten die Daten für vorgenannte Zwecke weitergeben (Art. 19 EU Data Act).

5 CLOUD SWITCHING

Mit dem EU Data Act werden Anbieter von Datenverarbeitungsdiensten (IaaS, PaaS, SaaS, XaaS) mit einer Vielzahl an Vorgaben dazu verpflichtet Massnahmen zu treffen, damit ihre Kunden nicht daran gehindert werden, zu einem anderen Anbieter, der vergleichbare Dienste erbringt, zu wechseln (re-sourcing) oder die Dienstleistungen inhouse zu verlegen (in-sourcing). Insbesondere dürfen Anbieter von Datenverarbeitungsdiensten keine vorkommerziellen, gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse für einen Wechsel (Switch) aufzwingen bzw. müssen solche Hindernisse beseitigen (Art. 23 ff. EU Data Act).

Die Pflichten des Anbieters, einen Lock-In des Kunden zu vermeiden, umfassen insbesondere:

- Kein Erschweren der Kündigung durch den Kunden (maximal 2 Monate Kündigungsfrist);
- Kein Erschweren des Wechsels zu einem anderen Anbieter;
- Inventar der zu übertragenden Daten und digitalen Assets;
- Sicherstellen der Übertragbarkeit (Portierung) der exportierbaren Daten (Input / Output, Metadaten, welche während der Vertragslaufzeit generiert worden sind;
- Sicherstellen der Übertragbarkeit durch Entbündeln der Services und Kompatibilität mit offenen Schnittstellen oder etablierten Interoperabilitätsstandards;
- Sicherstellen der Portierung innerhalb von 1 Monat (Verlängerung nur wenn dies durch den Anbieter begründet werden kann);
- Unterstützungsleistungen des Anbieters während dem Switch;
- Sicherstellen der Security während dem Switch;
- Sicherstellen der Kontinuität des Betriebs während dem Switch;
- Ab 11. Januar 2024 (Datum des Inkrafttretens des EU Data Act) müssen die obigen Leistungen zum Selbstkostenpreis erbracht werden, ab 12. Januar 2027 müssen diese vollständig gratis

erfolgen (Art. 29 EU Data Act), damit der Kunde nicht aufgrund hoher Vergütungen am Switching gehindert wird.

Art. 25 EU Data Act enthält konkrete Vorgaben, wie die Verträge der Anbieter von Datenverarbeitungsdiensten ausgestaltet werden müssen, damit die obigen Vorgaben eingehalten werden. Zudem müssen diese Anbieter den Kunden Informationen über die verfügbaren Verfahren und Methoden für den Switch und die Übertragung von Inhalten und Formaten sowie über bekannte Einschränkungen und technische Beschränkungen zur Verfügung stellen. Darüber hinaus sind die Anbieter von Datenverarbeitungsdiensten verpflichtet, ein aktuelles Online-Register der Anbieter von Datenverarbeitungsdiensten mit Einzelheiten zu allen Datenstrukturen und Datenformaten sowie zu den einschlägigen Normen und offenen Interoperabilitätsspezifikationen zu exportierbaren Daten abzugeben (Art. 26 EU Data Act).

Schliesslich müssen die Anbieter von Datenverarbeitungsdiensten auch vertragliche Transparenzpflichten in Bezug auf den Zugang und die Übermittlung im internationalen Umfeld einhalten, indem sie auf ihrer Website den Gerichtsstand angeben zusammen mit einer Beschreibung der technischen, organisatorischen und vertraglichen Massnahmen, die der Anbieter von Datenverarbeitungsdiensten getroffen hat, um einen internationalen staatlichen Zugang zu oder eine internationale staatliche Übermittlung von in der EU gespeicherten nicht-personenbezogenen Daten zu verhindern, wenn ein entsprechender Zugang oder eine entsprechende Übermittlung im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde.

6 EXTRATERRITORIALE WIRKUNG

Wie andere EU-Rechtsakte kommt auch dem EU Data Act extraterritoriale Wirkung zu (Auswirkungsprinzip). Somit gilt der EU Data Act gemäss Art. 1.3 auch für Anbieter in der Schweiz, wenn sie

- vernetzte Produkte in der EU (im EWR) in Verkehr bringen,
- verbundene Dienste an Nutzerinnen in der EU (im EWR) anbieten,
- Dateninhaber sind, die Daten an Empfängerinnen in der EU (im EWR) bereitstellen, oder
- Dienstleistungen zur Datenverarbeitung an Kunden in der EU (im EWR) erbringen (Cloud- und Edge-Dienstleistungen).

7 SANKTIONEN

Wir haben uns schon beinahe daran gewöhnt, dass jeder neue EU-Rechtsakt Klauseln enthält, wonach die zuständigen Behörden bei mangelnder Compliance mit den Vorgaben potentiell drakonische Unternehmensbussen verhängen dürfen. Der EU Data Act ist hier eine Ausnahme: Es sind die Mitgliedstaaten, die Vorschriften über Sanktionen erlassen sollen, die bei Verstössen gegen den EU Data Act zu verhängen sind. Der EU Data Act schreibt lediglich vor, dass diese Sanktionen wirksam, verhältnismässig und abschreckend sein müssen (Art. 41 EU Data Act). Insofern ergibt sich trotz der Harmonisierung, die der EU Data Act bezweckt (Erw. 4 EU Data Act), wiederum eine Fragmentierung.

8 ABGRENZUNGEN

Die nachstehenden Abgrenzungen sollen dem besseren Verständnis des EU Data Act und dessen Einbettung in weitere EU-Rechtsakte dienen:

1. Der EU Data Act verleiht keine ausschliesslichen Zugangs- oder Nutzungsrechte (Erw. 6).
2. Der EU Data Act verleiht einem Dateninhaber kein neues Recht auf Nutzung von Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert werden (Erw. 5 und 25).
3. Der EU Data Act schränkt den Schutz von Personendaten nach DSGVO und der Datenschutzrichtlinie 2002/58/EG für die elektronische Kommunikation nicht ein, sondern letztere haben Vorrang vor dem EU Data Act (Erw. 7).
4. Der EU Data Act hebt den datenschutzrechtlichen Grundsatz der Datenminimierung nicht auf (Erw. 20).
5. Der EU Data Act stellt keine Rechtsgrundlage für die Erhebung, Verarbeitung oder Weitergabe (Bekanntgabe) von personenbezogenen Daten dar (Erw. 7).
6. Regularien über die Herstellung und Sicherheit von Produkten bleiben vom EU Data Act unberührt (Erw. 11).
7. Die Bestimmungen über geistiges Eigentum der EU und der Mitgliedstaaten bleiben vom EU Data Act weitgehend unberührt und geistiges Eigentum soll geschützt bleiben (Erw. 13 und 16, siehe aber die Einschränkung des Schutzrechts sui generis für Datenbanken nach Art. 7 der Richtlinie 96/9/EG des Europäischen Parlaments in Art. 43 EU Data Act).
8. Für den Schutz von Nutzerinnen, die Verbraucherinnen sind, gilt weiterhin der Verbraucherschutz. Zum Schutz vor missbräuchlichen Vertragsklauseln zwischen einem Dateninhaber und einer Verbraucherin als Nutzerin eines vernetzten Produkts oder verbundenen Dienstes, gelten insbesondere die Richtlinien 93/13/EWG und 2005/29/EG (Erw. 9 und 28).
9. Geschäftsgeheimnisse sollen trotz des Datenzugangs und der Datenweitergabe weiterhin geschützt bleiben.
10. Zugangs- und Weitergaberechte, die in anderen EU-Rechtsakten enthalten sind und bereits vor dem Inkrafttreten des EU Data Act erlassen wurden, sollen vom EU Data Act unberührt bleiben (Art. 44 EU Data Act).

9 WÜRDIGUNG

Die Bedeutung des EU Data Act darf nicht unterschätzt werden. Nutzerinnen sollen selbstbestimmt entscheiden, was mit ihren Daten passiert und damit die «Datenschatztruhen öffnen», die den Nutzerinnen und Dritten bislang weitgehend verschlossen blieben. Mit dem EU Data Act soll kein neues absolutes Recht und schon gar kein Eigentumsrecht an Daten geschaffen werden, denn der EU Data Act klärt die Rechtsnatur der Ansprüche ebensowenig wie andere Regularien (wie etwa der EU Data Governance Act). Aber die Zuordnung von nicht-personenbezogenen Daten zu einer Nutzerin ist ebenso neu wie auch die grundsätzliche Nutzerzentrierung. Dreh- und Angelpunkt des EU Data Act betreffend Datenzugang und Datenweitergabe ist die Nutzerin: Nur die Nutzerin kann Zugang zu den Daten verlangen, die durch die Nutzung eines IoT-Produkts generiert werden, und zwar entweder für sich selbst (Art. 4.1 EU Data Act) und / oder für einen Dritten (Art. 5.1 EU Data Act), wobei jeder Zugriff eines Dritten somit von der Nutzerin abhängig ist. Dateninhaber sollten Dritten nicht-personenbezogene Produktdaten weder zu kommerziellen noch zu nichtkommerziellen Zwecken bereitstellen, ausser es geht um die Erfüllung ihres Vertrags mit der

Nutzerin (Erw. 26). Dieser Ansatz, der die Nutzerin in den Mittelpunkt stellt, ist bemerkenswert. Ob die Nutzerin damit so ermächtigt wird (vgl. Erw. 19), wie sich die EU dies vorstellt, wird sich weisen müssen. Denkbar ist auch, dass Nutzerinnen von Herstellern und Dateninhabern weiterhin primär als «blosse Datenproduzentinnen» wahrgenommen werden. Zudem wird das Datenportabilitätsrecht nach DSGVO von den betroffenen Personen bis heute noch kaum genutzt. Es bleibt abzuwarten, ob das Datenportabilitätsrecht (Datenweitergaberecht) nach dem EU Data Act grössere Wirkung erzielen wird und damit die «Datenschutztruhen» geöffnet werden. Jedenfalls hat der EU Data Act unmittelbare Auswirkungen darauf, wie vernetzte Produkte und verbundene Dienste konzipiert werden. Zudem werden auch die Informationspflichten umgesetzt werden müssen, die sich bislang im Falle der Bearbeitung von Personendaten auf Datenschutzerklärungen beschränkten. Umfassendere Information der Nutzerinnen ist in der datengetriebenen Welt von heute sicherlich zu begrüssen.

Beim Zugangsrecht der öffentlichen Stellen zeigt sich ein gewisses Misstrauen gegenüber dem Staat (bzw. auch gegenüber der EU-Kommission, der Europäischen Zentralbank und sonstigen EU-Einrichtungen). Zwar geniesst eine öffentliche Stelle wie Private ein Datenzugangsrecht und Datenweitergaberecht, sofern sie selber Nutzerin eines vernetzten Produkts oder eines verbundenen Dienstes ist (Erw. 18 EU Data Act). Ist sie keine Nutzerin, sind ihre Zugangsrechte ausserordentlich beschränkt und sie trägt eine weitgehende Beweislast für die Legitimität ihres Zugangsgesuchs.

Schliesslich gibt es offene Fragen betreffend Abgrenzung von der DSGVO zu klären: Der EU Data Act regelt den Datenzugang und die Datenweitergabe sowohl von personenbezogenen als auch von nicht-personenbezogenen Daten. Der EU Data Act darf jedoch nicht so ausgelegt werden, dass das Recht auf den Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation abgeschwächt oder eingeschränkt wird, weshalb solche Bestimmungen dem EU Data Act vorgehen (Erw. 7 EU Data Act). Hier dürften sich in der Praxis schwierige Abgrenzungsfragen ergeben, nicht zuletzt auch aufgrund des Umstands, dass sich in diversen Konstellationen die Dichotomie personenbezogen – nicht-personenbezogen zusehends auflöst oder in bestimmten Bereichen keine Trennung mehr möglich ist. Trotz des Gebots des Vorrangs von datenschutzrechtlichen Bestimmungen löst der EU Data Act das Verhältnis zum und das Zusammenspiel mit dem Datenschutzrecht / Grundrecht auf Privatsphäre nicht wirklich. Unklarheiten ergeben sich daraus, dass sich die Datenweitergabe (Bekanntgabe) im Zusammenhang mit Personendaten an die datenschutzrechtlichen Vorgaben halten muss. Dies gilt insbesondere auch dann, wenn ein Nutzer, der den Datenzugang oder die Datenweitergabe verlangt, nicht die betroffene Person ist, deren Personendaten bei der Nutzung des vernetzten Produkts generiert werden.

Das Eingreifen in die Vertragsfreiheit zugunsten der schwächeren Partei (B2C) ist bereits aus dem Verbraucherschutzrecht bekannt (https://commission.europa.eu/strategy-and-policy/policies/consumers_de). Der EU Data Act greift nun aber neu auch in die Vertragsfreiheit von Unternehmen (B2B) ein und will neu auch Unternehmen vor missbräuchlichen oder diskriminierenden Vertragsklauseln schützen. Dies stellt eine ordnungspolitische Massnahme dar, welche wohl durch die AGB-Politik grosser (Tech-)Unternehmen beeinflusst wurde, die den Kundinnen wenig bis gar keinen Spielraum bieten, Verträge oder wenigstens bestimmte Vertragsklauseln individuell zu verhandeln. Grundsätzlich ist der Gedanke, die schwächere Partei vor missbräuchlichen Vertragsbedingungen schützen zu wollen, zu begrüssen: meist verfügen sie nicht über die Ressourcen, um sich gegen einen Anbieter durchzusetzen, der mittels AGB die Vertragsbedingungen für alle seine Vertragspartner diktieren kann. Allerdings sind von

diesen Vorgaben sämtliche Anbieter betroffen, und damit auch kleinere, die ihre Vertragsbedingungen nun auf eigene Kosten anpassen müssen.

Insbesondere hinsichtlich der Vorgaben für Cloud-Switching trifft der EU Data Act keine Unterscheidung zwischen kleinen und grossen Anbietern und nimmt nicht nur Hyperscaler in die Pflicht. Für sämtliche Anbieter bedeutet die Compliance mit den Vorgaben Aufwand und Kosten, ihre AGB abzuändern. Dass aber die Leistungen für den Wechsel ab 11. Januar 2024 zum Selbstkostenpreis und ab 12. Januar 2027 vollständig gratis zu erfolgen haben, bedeutet, dass die entsprechenden Kosten und Aufwände bereits in das Pricing der Leistungen während der Dauer des Vertrags einkalkuliert werden wird, was die ohnehin häufig hohen Preise für Cloud-Dienstleistungen nochmals erhöhen wird. Zudem ist zu bedenken, dass Cloud-Switching für alle Beteiligten (Kunde, alter Anbieter, neuer Anbieter) mit viel Aufwand und Unwägbarkeiten verbunden ist. Insbesondere hat ein alter Anbieter keinerlei Einfluss darauf, wie viel Aufwand der Kunde und der neue Anbieter beim Switching generieren könnten. Der EU Data Act sieht hierfür keine Bestimmungen vor, die den alten Anbieter schützen würden – ausser dass sich alle Beteiligten nach Treu und Glauben verhalten sollen (Art. 27 EU Data Act), was kaum vor Zusatzaufwänden schützen wird.

Zudem soll die EU-Kommission unverbindliche Mustervertragsklauseln für die Datenweitergabe zwischen Unternehmen erarbeiten, die den Parteien beim Vertragsdrafting helfen sollen und die «bargaining power» der Nutzerinnen bzw. Kundinnen verbessern sollten. Auch soll die EU-Kommission nicht-verbindliche Standardvertragsklauseln für Verträge über Cloud-Computing erarbeiten, um das Cloud-Switching zu erleichtern (Art. 41 EU Data Act). Die EU-Rechtsakte der jüngsten Vergangenheit sehen vermehrt von der EU-Kommission zu erlassende Muster- oder Standardvertragsklauseln vor. Angesichts der teilweise durchwachsenen Qualität dieser Muster- oder Standardvertragsklauseln kann dieser Entwicklung bestenfalls mit gemischten Gefühlen begegnet werden. Insbesondere, wenn diese punktgenau ihr Ziel verfehlen, indem sie die zu schützende Partei schwächen. Mit einem solchen Bärendienst wird es in Vertragsverhandlungen künftig nur noch schwieriger, sinnvolle Vertragsklauseln verhandeln zu können.

Ferner werden im Zusammenhang mit den Vorgaben für das Cloud-Switching die unter der DSGVO eingeführten Regeln für den internationalen Transfer bzw. die Verhinderung des Zugriffs auf personenbezogene Daten von ausserhalb der EU wenigstens im Grundsatz auf nicht-personenbezogene Daten ausgeweitet. Dies mag den Schutz von Sachdaten, insbesondere von Geschäftsgeheimnissen, zwar erhöhen, kann aber auch als Hindernis für den weltweiten Datenfluss erachtet werden. Zudem dürfte hier wiederum ein ordnungspolitisches Ziel durchschimmern, welches auf US Techfirmen fokussiert, das aus Sicht vieler Kunden im EWR nicht unbedingt erwünscht ist.

Trotz aller Kritik dürften Kundinnen in der Schweiz von diesen vertraglichen Vorgaben wohl ebenfalls profitieren, ist doch nicht einzusehen, weshalb Anbieter die Schweizer Kundinnen gegenüber Kundinnen im EWR benachteiligen sollten. Denkbar ist einzig, dass ausländische Anbieter sich Zeit lassen, ihre AGB für die Schweiz anzupassen.

10 UND DIE SCHWEIZ?

Mit der «Strategie Digitale Schweiz 2023» vom 11. September 2020 wurde das Konzept der «vertrauenswürdigen Datenräume basierend auf der digitalen Selbstbestimmung» erstmals auf

Bundesebene eingeführt. Aktuell wird eine Auslegeordnung zum Entwurf eines Rahmengesetzes über die Sekundärnutzung von Daten erarbeitet, welches die schweizweite Mehrfachnutzung von Daten adressieren soll, damit Infrastrukturen für die Sekundärnutzung von Daten in strategisch relevanten Bereichen rasch initialisiert und aufgebaut werden können. Die geregelte Sekundärnutzung von Daten, insbesondere die Verknüpfung von Daten, ist eine zentrale Grundlage für den Aufbau und die Umsetzung des Schweizer Datenökosystems (vgl. Diskussionspapier «Schweizer Datenökosystem» Aufbau und Weiterentwicklung des Schweizer Datenökosystems und der dazugehörigen Datenaustauschinfrastrukturen, Bundeskanzlei, Digitale Transformation und IKT Lenkung (DTI), 31. Januar 2023, Seite 10).

Im Rahmen der Auslegeordnung wurde eine Analyse bestehender Datenräume, Komponenten und Services durchgeführt. Dies sind beispielsweise der Linked Data Service LINDAS des Bundesarchivs, das Vorhaben der Nationalen Datenbewirtschaftung NaDB des Bundesamtes für Statistik, die Plattform opendata.swiss, das Geoportal des Bundes oder die Nationale Datenvernetzungsinfrastruktur Mobilität NADIM des Bundesamtes für Verkehr.

Es gibt in der Schweiz (noch) keine kohärente Datenpolitik oder Digitalisierungspolitik, die sich mit dem EU-Binnenmarkt für Daten messen lassen könnte. Auch bestehen in der Schweiz abgesehen von EMBAG und EPDG (noch) keine horizontalen Regeln oder Gesetze zur Gouvernanz von Sachdaten.