4/2023
73 – 96

EuGH
Österreichische Post
Thomas Schweiger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Künstliche Intelligenz und Datenschutz

Europa setzt Maßstäbe im KI-Recht

Interview mit Martin Selmayr, EK

DGA, DMA, DSA, DA, AI Act, EHDS – ein Überblick (Teil 2)

Rainer Knyrim und Lena Urban

Was ist der EDHS?

Michael Löffler und Markus Kastelitz

AI Act: Das Ende der Innovation oder Gefahr für den Datenschutz?

Tünde Fülöp

ChatGPT und Mitarbeiter:innen – ein Risiko?

André Rohrleitner

Checkliste: KI und Datenschutz

Hans-Jürgen Pollirer

ISSN 2313-5409

dako.manz.at

MANZ

Rainer Knyrim/Lena Urban
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte/Rechtsanwältin in Kooperation bei Knyrim Trieb Rechtsanwälte

DGA, DMA, DSA, DA, AI Act, EHDS – ein Überblick über die europäische Datenstrategie (Teil 2)

DGA, DMA, DSA, DA, AI Act, EHDS, Datenstrategie. Seit 2022 geht es Schlag auf Schlag: Alle paar Monate erlässt die EU einen neuen Rechtsakt, der die Verarbeitung von Daten aus unterschiedlichen Gesichtspunkten regelt. Dieser zweite Teil des Beitrags gibt einen Überblick über DA, AI-Act und EHDS.

Data Act

Der erste Vorschlag 2022/0047 zum Data Act (Datengesetz, kurz „DA") stammt vom 23. 2. 2022, am 27. 6. 2023 wurde ein politischer Konsens zwischen dem Europäischen Rat, EP und EK erzielt, auf dem die nachstehenden Ausführungen basieren.[1]

Die **Publikation** des Data Acts im Amtsblatt wird dementsprechend in den nächsten Wochen erwartet. Die Anwendbarkeit ist knapp 21 Monate danach geplant, also voraussichtlich im Frühling/Sommer 2025. Der Datenzugang muss allerdings schon nach einem Jahr bestehen, also voraussichtlich schon im Herbst 2024.

Regelungsgegenstand

Der DA wird einer der spannendsten und wichtigsten Regelwerke zum Datenzugang und zur Datennutzung sein, soll er doch einen **Ferndatenzugang** und eine **faire Datennutzung** hinsichtlich von Daten, die bei Nutzung eines Gerätes oder verbundenen Dienstes erzeugt werden, schaffen. Er zielt damit direkt auf **Datenanwendungen** der **Industrie** oder des **Internet of Things** ab und ebenso auf Services, die Daten produzieren.

Die **DSGVO** soll durch den DA **nicht berührt** werden, durch den DA werden die Bestimmungen des Art 20 DSGVO zur Datenportabilität aber ergänzt. Nach der Definition des DA sind Daten jede digitale Darstellung von Handlungen, Tatsachen, Informationen, und dies unabhängig vom Personenbezug.

Regelungsadressaten des DA sind Hersteller von vernetzten Produkten, Erbringer von damit zusammenhängenden Dienstleistungen, aber ebenso Nutzer, Dateninhaber, Datenempfänger, Anbieter von Datenverarbeitungsdiensten, öffentliche Einrichtungen und Betreiber von Datenräumen.

Kostenloser Datenzugriff in Echtzeit

Der Data Act soll den Nutzern von vernetzten Geräten und damit zusammenhängenden Diensten, die Daten erzeugen, **umfangreiche Rechte** auf Datennutzung einräumen und Datenzugriff direkt auf das Produkt oder über Schnittstellen, und dies kostenlos und gegebenenfalls in Echtzeit in einem gängigen, maschinenlesbaren Format ermöglichen. Weiters soll es den Usern möglich sein, die **Daten mit Dritten** zu **teilen**. Wenn die Nutzer nicht die betroffenen Personen selbst sind und es sich um personenbezogene Daten handelt, muss die Einwilligung der betroffenen Personen vorliegen.

Den Herstellern bzw Vertragspartnern des Nutzers wird die Verpflichtung auferlegt, die Produkte und Dienstleistungen so zu designen, dass diese einfach, sicher und – soweit relevant und angemessen – direkt den Zugang zu den Daten ermöglichen („**Data Accessibility by Design**"). Weiters sollen die Hersteller zu **vorvertraglichen Informationsverpflichtungen** ähnlich Art 13 DSGVO verpflichtet werden und über die verarbeiteten Daten sowie Zugriffsmöglichkeiten sowie Weitergabemöglichkeiten informieren.

Dateninhaber sollen ihrerseits wieder verpflichtet werden, Daten auf Verlangen des Nutzers an Dritte zur Verfügung zu stellen, wobei dies bei personenbezogenen Daten nur mit Einwilligung geschehen soll, was eine Erweiterung von Art 20 DSGVO, aber ohne Rücksicht auf die technische Machbarkeit dieser Zur-Verfügung-Stellung bedeutet.

Bei der **Herausgabe von Daten** durch Dateninhaber kann eine **Gegenleistung** für die Bereitstellung der Daten verlangt werden, diese muss jedoch zu sog „FRAND"-Bedingungen (fair, reasonable and non-discriminatory; also fair, angemessen und nichtdiskriminierend) erfolgen. Weiters müssen **technische Schutzmaßnahmen** gegen unerlaubten Datenzugriff implementiert werden und im Fall von Streitigkeiten soll es eine **Streitbeilegungsstelle** geben.

Es wird unzulässig sein, missbräuchliche Klauseln zu verwenden, va hinsichtlich Ausschlusses und Beschränkung von Haftung, Rechtsbehelfen, verhältnismäßiger Datennutzung oder zu kurzer Kündigungsfristen.

Sonderregelungen gibt es für den Fall eines öffentlichen Notstandes, bei denen öffentliche Stellen von privatwirtschaftlichen Unternehmen Daten herausverlangen können, falls die Daten nicht auf dem Markt zu Marktpreisen erhältlich sind und diese unverzüglich erforderlich sind.

Interoperabilität

Der Entwurf enthielt auch einen eigenen Abschnitt zum Wechsel zwischen Datenverarbeitungsservices. Es sollte möglich sein, einen Wechsel zum gleichen Service-Typ oder auf einer On-Premise-Variante durchzuführen, und dabei sollten **keine Wechselgebühren** verlangt werden dürfen. Im politischen Konsens wurden diese Bestimmungen anscheinend wieder entfernt und dieser sieht nun nur mehr vor, dass Datenräume eine Reihe von Interoperabilitätsanforderungen erfüllen müssen.

Interessant ist, dass der Vorschlag des DA – genauso auch wie der DGA – **Sonderregelungen** für die internationale Datenübertragung in Drittstaaten enthält. Diese Regeln erinnern etwas an die Regeln in der DSGVO und dürften Ausfluss des *Schrems II*-Urteils des EuGH sein,[2] dessen Gedanken hier auch auf nicht-personenbezogene Daten ausgeweitet werden (bei personenbezogenen Daten ist jedenfalls die DSGVO zu beachten).

Bedeutung des DA

Wie schon ausgeführt ist der DA wichtig für Industriedaten und Internet-of-Things-Anwendungen, wobei dieses Thema sehr

[1] Vorschlag des Europäischen Rates 7413/23 vom 17. 3. 2023, Stand 27. 6. 2023. [2] EuGH 16. 7. 2020, C-311/18.

komplex ist. Die Praxis zeigt heute schon, dass es teilweise **mehrschichtige Konstellationen** mit Herstellern, Verleihern und Kunden gibt, die alle Daten etwa aus Fahrzeugen[3] oder Geräten nutzen wollen und womöglich auch zu Geld machen wollen, gleichzeitig aber die Privatsphäre der Enduser oder auch der die Geräte oder Fahrzeuge bedienenden Mitarbeiter zu berücksichtigen sind, wie auch der in Österreich besondere Schutz von Firmendaten nach § 1 DSG. Die hier vorliegenden unterschiedlichen Interessenlagen aufzulösen ist bereits heute sehr schwierig und wird durch den DA noch komplexer werden.

Sanktionen

Der Entwurf des DA sieht die Möglichkeit der **Kompetenzaufteilung** auf verschiedene Behörden vor. Hinsichtlich der Datennutzung sollen die nationalen Datenschutz-Aufsichtsbehörden zuständig sein, die Strafen wie unter der DSGVO verhängen können sollen, also bis zu 4% des weltweiten Konzernumsatzes des Vorjahres.

AI Act

Der Artificial Intelligence Act (Gesetz über künstliche Intelligenz, kurz „AI Act") ist derzeit ebenso noch im **Entwurfsstadium**. Der erste Vorschlag 2021/0106 stammt vom 21. 4. 2021. Auch zum AI Act wurden zwischenzeitlich weitere Textvorschläge veröffentlicht, der letzte zum Zeitpunkt der Drucklegung dieses Beitrags war die Position des EP vom 14. 6. 2023.[4] Auch für den AI Act wird eine **Finalisierung** noch im Jahr 2023 erwartet. Angesichts der Aktualität des Themas und der rasanten technischen Entwicklung ist aber auch denkbar, dass sich die Verabschiedung aufgrund erforderlicher Änderungen noch weiter verzögern wird, wobei gerade beim AI Act eine möglichst rasche Umsetzung wünschenswert wäre.

Regelungsgegenstand

Der AI Act soll im Wesentlichen **Verbots- und Produktsicherheitsvorschriften** für **künstliche Intelligenz** (KI) enthalten. Am Rande werden auch innovationsfördernde Maßnahmen geregelt.[5] Der Entwurf bezieht sich daher auf das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI. Regelungsadressaten sind daher insb Anbieter und Nutzer von KI.

Der Verordnungsvorschlag verfolgt einen **risikobasierten Ansatz**, wonach je nach Risiko, das mit dem KI-System verbunden ist, besondere Regeln gelten bzw das KI-System sogar verboten wird, wie bspw im Fall von Social Scoring in bestimmten Fällen. Insb die Definition eines KI-Systems ist umstritten. Im Vergleich zum Entwurf aus dem Jahr 2021 enthält der aktuellste Entwurf auch hier Änderungen. Darüber hinaus wird im Entwurf ein Kapitel zu *„KI mit allgemeinem Verwendungszweck"* vorgeschlagen, um KI wie bspw ChatGPT, die keine eindeutige Zweckbestimmung haben, besser mit der geplanten Regelung zu erfassen.

Hochrisiko-KI-Systeme

Der AI Act sieht insb für Hochrisiko-KI-Systeme spezielle Regeln vor. Als Hochrisiko-KI-System wird zum Beispiel ein System eingestuft, das für die Strafverfolgung oder für die Rechtspflege und demokratische Prozesse verwendet wird.

Hochrisiko-KI-Systeme müssen insb **Regelungen einhalten**, die sich bereits auf die **Entwicklung des Systems beziehen**. Bspw gibt es Qualitätskriterien für Trainings-, Validierungs- und Testdatensätze. Ferner gibt es Aufzeichnungspflichten und eine Informationspflicht an Nutzer, denen eine Art Gebrauchsanweisung zur Verfügung zu stellen ist. Die Möglichkeit der Beaufsichtigung durch natürliche Personen muss gegeben sein.

Aber auch für Nutzer werden Pflichten festgelegt. Diese müssen sich bspw an die Gebrauchsanweisung halten und in bestimmten Fällen den Händler oder Anbieter informieren sowie Protokolle über die Nutzung aufbewahren.

Transparenzpflichten und weitere geregelte Aspekte

Gegenüber Menschen, die mit einer KI interagieren, gelten gewisse Transparenzpflichten. Insb muss dem Menschen offengelegt werden, dass er mit einer KI interagiert.

Ferner wird im Verordnungsvorschlag die Möglichkeit von sog KI-Reallaboren **(Regulatory Sandboxes)** vorgesehen. Für Kleinanbieter und Kleinnutzer soll es besondere Hilfestellung geben.

Die MS müssen nach dem Verordnungsvorschlag eine **nationale Aufsichtsbehörde** benennen bzw einrichten.

Sanktionen

Die Sanktionen sind gestaffelt, im ursprünglichen Entwurf der EK je nach Verstoß zwischen 2% des weltweiten Vorjahresumsatzes und 10 Mio Euro und 6% des Vorjahresumsatzes und 30 Mio Euro, im Vorschlag des EP zwischen 1% bzw 1 Mio und 7% bzw 40 Mio Euro.

Bedeutung des AI Acts

Angesichts der aktuellen technischen Entwicklung ist der AI Act **besonders umstritten**. Wann es tatsächlich zu einer Finalisierung im Gesetzgebungsprozess kommen wird, ist aus heutiger Sicht noch unklar.

Kritisiert wird im bisherigen Vorschlag insb die recht weit gestaltete Definition der KI.[6] Darüber hinaus regelt der AI Act nicht alle Aspekte der Entwicklung und Nutzung von KI, sondern beschränkt sich im Wesentlichen auf Produktsicherheitsvorschriften für KI. Va für die Frage der Haftung gibt es im Entwurf keine Regelungen[7] und darüber hinaus werden auch keine besonderen Rechtsschutzinstrumente für Betroffene vorgesehen. Es bleibt abzuwarten, inwiefern sich das im Gesetzgebungsprozess möglicherweise noch ändert.

EHDS

Beim European Health Data Space („EHDS") bzw Europäischen Raum für Gesundheitsdaten handelt sich um einen Vorschlag für eine EU-VO vom 3. 5. 2022, der sich aktuell im **Gesetzgebungsprozess** befindet. Es soll sich dabei um einen mehrerer „gemeinsamer Europäischer Datenräume" im Rahmen der europäischen Datenstrategie handeln.[8]

Regelungsgegenstand

Der EHDS zielt darauf ab, dass eine **bessere Primär- und Sekundärnutzung** von elektronisch **vorhandenen Gesundheitsdaten** ermöglicht wird. In den Anwendungsbereich fällt die Verarbeitung elektronischer Gesundheitsdaten von Unionsbürgern und von Drittstaatsangehörigen mit

[3] Siehe *Wienroeder*, Der Entwurf des Data Act – Auswirkungen auf die Automobilindustrie, RAW 2022, 99.
[4] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM[2021] 0206 – C9-0146/2021 – 2021/0106[COD]), P9_TA(2023)023t.
[5] Siehe *Botte*, Die Förderung innovativer KI-Systeme in der EU, ZfDR 2022, 391.
[6] Siehe dazu zB *Bomhard/Merkle*, Europäische KI-Verordnung, RDi 2021, 276 (277).
[7] Von der Regelung iZm KI-Reallaboren abgesehen; für die allgemeine Frage der Haftung gibt es aktuell einen Vorschlag für eine EU-RL: Vorschlag für eine RL des europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche Haftung an künstliche Intelligenz (RL über KI-Haftung) 2022/0303 vom 28. 9. 2022.
[8] *Raji*, Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space, ZD 2023, 3.

Wohnsitz in der EU. Zudem gibt es Regelungen für Hersteller und Anbieter von sogenannten EHR-Systemen **(Systeme für elektronische Patientenakten)**.

Unter den Schlagworten „MyHealth@EU" und „HealthData@EU" sollen grenzüberschreitende Infrastrukturen für die Primär- und Sekundärnutzung elektronischer Gesundheitsdaten geschaffen werden.

Primärnutzung

Im Rahmen der Primärnutzung (MyHealth@EU) soll es im Wesentlichen eine **grenzüberschreitende** elektronische **Nutzung von Patientendaten** geben können. Die betroffenen natürlichen Personen sollen dabei bspw ein umfassendes Zugriffsrecht, ein Recht auf eine elektronische Kopie und auch die Möglichkeit zur Eingabe eigener Daten haben. Angehörige der Gesundheitsberufe können nach dem Verordnungsvorschlag Zugriff auf elektronische Gesundheitsdaten bekommen.

Der Verordnungsvorschlag sieht auch die Möglichkeit der EK vor, für Kategorien von Gesundheitsdienstleistern die Pflicht zur elektronischen **Registrierung von Gesundheitsdaten** vorzusehen. Abgesehen von dieser Möglichkeit sollen Angehörige der Gesundheitsberufe nur im Fall der elektronischen Verarbeitung von Gesundheitsdaten diese (sofern sie unter bestimmte Kategorien, die im Verordnungsvorschlag festgelegt sind, fallen) systematisch in einem elektronischen Format in einem EHR-System registrieren müssen. Hierunter fallen Daten wie bspw Patientenkurzakten, elektronische Verschreibungen, medizinische Bilder und Bildbefunde, Laborergebnisse.

Sekundärnutzung

Die geplante Regelung für die Sekundärnutzung elektronischer Gesundheitsdaten (HealthData@EU) zielt darauf ab, dass elektronische **Gesundheitsdaten** in verschiedensten Bereichen, wie insb im **Forschungsbereich** oder auch zum **KI-Training, weiterverwendet** werden können. Für bestimmte Zwecke, wie bspw für Entscheidungen zum Schaden einer natürlichen Person, soll die Verwendung der elektronischen Gesundheitsdaten allerdings untersagt sein. Der Verordnungsvorschlag sieht ein antragsgebundenes Verfahren vor, bei dem eine sog Zugangsstelle für Gesundheitsdaten, die von den MS eingerichtet werden muss, eine Datengenehmigung erteilt und dann in weiterer Folge die elektronischen Gesundheitsdaten vom Dateninhaber erhält und dem Antragsteller darauf Zugriff gewährt.

Bedeutung des EHDS

Erfreulich ist der von der EU gewählte Ansatz, nicht nur die Primärnutzung, sondern auch die Sekundärnutzung dieser Daten zu fördern.

Der Verordnungsvorschlag sieht lediglich vor, dass die DSGVO unberührt bleibt. Das genaue Verhältnis zu den Bestimmungen der DSGVO klärt der Verordnungsvorschlag jedoch nicht.[9] Zu befürchten ist ua, dass für Gesundheitsdiensteanbieter mit einem höheren Verwaltungsaufwand und höheren Kosten gerechnet werden muss.

Kritik wird am Verordnungsvorschlag auch deshalb geübt, weil Patienten keine Möglichkeit haben, um aus dem System hinauszuoptieren. Auch die Anonymisierung im Rahmen der Sekundärnutzung kann nicht in allen Fällen sichergestellt werden.

Sanktionen

Die Sanktionen sollen von den MS selbst bestimmt werden und müssen wirksam, verhältnismäßig und abschreckend sein.

Dako 2023/40

[9] Siehe zum Beispiel *Raji*, ZD 2023, 3 (8).

Zum Thema

Über den Autor und die Autorin

Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte in Wien. E-Mail: ky@kt.at

Mag.[a] Lena Urban ist Rechtsanwältin in Kooperation bei Knyrim Trieb Rechtsanwälte in Wien. E-Mail: lu@kt.at

Hinweis

Teil 1 dieses Beitrags zum DMA, DGA und DSA ist erschienen in Dako Heft 3/2023 (Dako 2023/30).

Impressum gem. § 24 MedienG

Offenlegung gem. § 25 MedienG und Angaben zu § 5 ECG abrufbar unter https://www.manz.at/impressum

Medieninhaber und Herausgeber: MANZ'sche Verlags- und Universitätsbuchhandlung GmbH. **Anschrift:** Kohlmarkt 16, 1010 Wien. **Verlagsadresse:** Johannesgasse 23, 1010 Wien (verlag@manz.at). **Redaktion:** Dr. Rainer Knyrim (Chefredakteur); Mag. Viktoria Haidinger, LL.M.; DI. Michael Löffler; Prof. KommR Hans-Jürgen Pollirer, Ing. Dr. Christof Tschohl. **E-Mail:** dako@manz.at **Verlagsredaktion:** Dr. Elisabeth Maier, Johannesgasse 23, 1010 Wien, E-Mail: elisabeth.maier@manz.at **Hersteller:** Printera Grupa d.o.o., 10431 Sveta Nedelja. **Herstellungsort:** Sveta Nedelja, Kroatien. **Verlagsort:** Wien, Österreich. **Zitiervorschlag:** Dako 2023/Nummer. **Anzeigenkontakt:** Stefan Dallinger, Tel: (01) 531 61-114, Fax: (01) 531 61-596, E-Mail: stefan.dallinger@manz.at **Bezugsbedingungen:** Die Dako erscheint 5 × jährlich. Der Bezugspreis 2023(10. Jahrgang) beträgt € 179,– (inkl Versand in Österreich). Einzelheft € 43,00. Auslandspreise auf Anfrage. Nicht rechtzeitig vor ihrem Ablauf abbestellte Abonnements gelten für ein weiteres Jahr als erneuert. Abbestellungen müssen schriftlich bis spätestens 18. November des laufenden Abojahres beim Verlag einlangen. **Formatvorlagen:** Zum Download unter www.manz.at/formatvorlagen **Hinweis:** Auf eine geschlechtergerechte Sprache wird geachtet. Wird jedoch von einzelnen Autoren zugunsten der leichteren Lesbarkeit bloß die männliche oder die weibliche Form verwendet, sind immer beide Geschlechter gleichermaßen gemeint. **AZR:** Alle Abkürzungen entsprechen den „Abkürzungs- und Zitierregeln" (AZR), 8. Aufl (Verlag Manz, 2019). **Grafisches Konzept:** Michael Fürnsinn für buero8, 1070 Wien (buero8.com).