AK EUROPA

Positionspapier
August 2022
Konsument:innen

COM(2022) 197

Verordnung über den europäischen Raum für Gesundheitsdaten

Analysen aus sensiblen Gesundheitsdaten sind auch ohne Aufweichen von Datenschutzrechten möglich!

Zusammenfassung

Der Verordnungsentwurf bezweckt,

- „Akteuren aus Forschung und Innovation, politischen Entscheidungsträgern und Regulierungsbehörden" EU-weiten Zugang zu elektronischen Gesundheitsdaten zu verschaffen. Öffentliche wie private „Dateninhaber" werden verpflichtet, für Zwecke der Gesundheitsversorgung erhobene Daten an eine „Zugangsstelle" für Gesundheitsdaten herauszugeben, die diese Datennutzern auch in pseudonymisierter (mittelbar personenbezogener) Form EU-weit anbietet.
- die Gestaltung eines „echten Binnenmarktes für datenbasierte digitale Gesundheitsprodukte und -dienste" und
- einen leichteren Zugang natürlicher Personen zu ihren im Zuge der Gesundheitsversorgung anfallenden elektronischen Gesundheitsdaten.

Das Wichtigste in Kürze

- Gesundheitsdaten zusammenzuführen und wissenschaftlich auszuwerten kann dazu beitragen, Diagnostik und Therapien zu verbessern und gesundheitspolitische Weichenstellungen rascher und besser vorzunehmen. Die AK unterstützt daher grundsätzlich Bestrebungen, Gesundheitsdaten besser zu nützen. Wer, weshalb, wozu Zugang zur Nutzung von Gesundheitsdaten erhält, ist jedoch für Betroffene transparent zu regeln und hat unter Einhaltung des Datenschutzes zu erfolgen. Insbesondere ist jede Rückführbarkeit auf Einzelpersonen auszuschließen, sofern keine ausdrückliche Einwilligung zur Nutzung von Gesundheitsdaten vorliegt.
- Das Vorhaben ist grundrechtlich überaus brisant. Das vorliegende Positionspapier befasst sich mit den Auswirkungen des Projektes auf Konsument:innen/Patient:innen und ihrem Recht auf Datenschutz. Gesundheitspolitische Aspekte werden nicht berücksichtigt.
- Die Schutzstandards der Datenschutz-grundverordnung (DSGVO) werden unterschritten.
- Das Selbstbestimmungsrecht der von den beabsichtigten Verarbeitungen Betroffenen tritt pauschal und undifferenziert hinter die Verwertungsinteressen der Datenökonomie zurück.
- Betroffene könnten auf die Weiternutzung ihrer Gesundheitsdaten und eine Fülle weiterer Daten (gesundheitsbeeinflussende Faktoren wie individuelle Verhaltensweisen, Einkommen uvm) keinen Einfluss nehmen: ihnen stünde kein Einwilligungsrecht bzw Widerrufsrecht zu, obwohl ihre (mittelbar) personenbezogenen Daten für alle nur erdenklichen politischen, wissenschaftlichen und kommerziellen Projekte, an denen öffentliche Interessen bestehen bzw behauptet werden, ausgewertet werden dürfen.
- Betroffene wüssten nicht, wer, wo, welche Daten, wofür und wie lange verwendet. Geht es nach der Kommission, so entfällt nämlich die Informationspflicht nach der DSGVO darüber, wer, mit welchen Daten für welchen Zweck Datenanalysen durchführt. Lediglich auf Websites sind allgemeinste Informationen über erteilte Datengenehmigungen zu veröffentlichen. Das Recht aufgrund der DSGVO, detaillierte Auskunft verlangen zu können, wird nur bei der „primären Datennutzung" (für die Erbringung von Gesundheitsdiensten) explizit beschrieben. Bei der „sekundären Datennutzung" (Weiterverarbeitung für andere Zwecke) wird dieses Recht schon dadurch faktisch beschnitten, dass Betroffene nicht einmal erfahren, in welchen der Datengenehmigungen ihre Daten stecken.
- Der Schutz gegen Datenmissbrauch wird im Entwurf nicht nennenswert geregelt. Das ist ein grober Sorgfaltsmangel: zentral abrufbare Datenbestände dieser Größe und von hohem Handelswert samt EU-weiten Zugriffen ziehen fast zwangsläufig auch missbräuchliche, kriminelle Praktiken an.
- Eine seriöse Bewertung aller Folgen der VO wird dadurch erschwert, dass sich die Kommission an zahllosen Stellen im Entwurf für die technisch/organisatorische Umsetzung delegierte Akte vorbehält.

Die Position der AK

Forderungen aus Datenschutz- und Konsument:innen-Sicht

Die AK lehnt einen DSGVO-widrigen, weil undifferenzierten, pauschalen Vorrang der Datennutzung vor den Geheimhaltungsinteressen der Betroffenen ab. Will man das Vertrauen der Bevölkerung in die Nutzung ihrer Gesundheitsdaten etwa für Forschungszwecke stärken statt verlieren, ist ein Konzept nötig, das die DSGVO und insbesondere die Selbstbestimmung der Betroffenen achtet. Aufgrund seiner Eingriffstiefe in die Datenschutzrechte von Konsument:innen/Patient:innen/Bürger:innen ist der Europäische Datenschutzbeauftragte bzw Datenschutzausschuss einzubinden und der Entwurf elementar zu überarbeiten:

Der Datenumfang ist viel zu umfangreich und unbestimmt: Das Zusammenführen sämtlicher Daten aus dem Gesundheitsbereich mit allen nur erdenklichen sozio-demografischen Verhaltensdaten würde ein einzigartiges individuelles Verhaltensprofil ermöglichen, das bisherige kommerzielle Verhaltensprofile der Digitalwirtschaft in den Schatten stellt. Auch eine Blankoermächtigung für den Abgleich mit Daten aus allen anderen Lebensbereichen in völlig unspezifischen „Notsituationen" ist enthalten. Die Gesundheitsdaten, die für die Sekundärnutzung verarbeitet werden können, sollten „flexibel genug sein, um den sich wandelnden Bedürfnissen der Datennutzer gerecht zu werden, vor allem auch gesundheitsrelevante Einflussfaktoren umfassen" (siehe EG 39). Dazu zählen:

- Daten aus dem Gesundheitssystem, wie elektronische Patient:innenakten, Daten zu Krankenversicherungsleistungen, Krankheitsregister, Genomdaten usw.
- Daten zu gesundheitsrelevanten Einflussfaktoren wie z.B. Konsum bestimmter Substanzen, Obdachlosigkeit, Krankenversicherung, Mindesteinkommen, beruflicher Status, Verhalten.
- Auch von Personen selbst erzeugte Daten, z.B. Daten von Medizinprodukten, Wellness-Apps oder anderen tragbaren Geräten und digitalen Gesundheitsanwendungen, können dazugehören.
- Datennutzer dürfen die Daten auch mit ganz anderen Daten anreichern und sollten die „verbesserten" Datensätze dem ursprünglichen Dateninhaber kostenlos bereitstellen.
- Registerdaten, wie Impfregister uvm.

Wer "Dateninhaber" ist, der seine Daten für die Weiterverarbeitung anbieten muss, wird nicht präzisiert: Der Kreis der Adressaten ist nicht einigermaßen rechtssicher abgesteckt. Es könne sich um „öffentliche, nicht gewinnorientierte oder private Gesundheits- und Pflegedienstleister, um öffentliche, nicht gewinnorientierte oder private Organisationen, Verbände oder andere Einrichtungen oder um öffentliche und private Forschungseinrichtungen im Gesundheitsbereich handeln.

Ein Rückschluss auf bestimmbare Einzelpersonen ist möglich: Betroffene müssten damit rechnen, dass sensibelste Daten, ganze Verhaltens- und Gesundheitsprofile sowie Zusammenhänge und Analysen daraus ihrer Person konkret zuordenbar sind. Der Entwurf enthält nicht nur keine diesbezügliche Schutzgarantie. Einzelne Bestimmungen und EG gehen dezidiert davon aus, dass die Zugangsstellen zu Gesundheitsdaten, den Datenzugang in einer Weise ermöglichen, dass Rückschlüsse auf einzelne Personen denkbar sind.

In einigen Fällen könnten die Informationen zu bestimmten natürlichen Personen
(z.B. Genomdaten natürlicher Personen mit einer bestimmten Krankheit) – führt die Kommission bspw in EG 41 aus – die Diagnose oder Behandlung anderer Personen unterstützen. Und weiter: „Jedes Bestreben, die Daten für Maßnahmen zum Nachteil der betroffenen Person zu verwenden, Versicherungsbeiträge zu erhöhen, Produkte oder Behandlungen zu bewerben oder schädliche Produkte zu entwickeln, sollte verboten werden" (siehe Art 35 und EG 41). Dieser Klarstellungen bzw Verwendungsverbote bedürfte es nicht,

würde die Kommission darauf vertrauen, dass ein Rückschluss auf bestimmte Personen im Zuge der Weiterverarbeitung pseudonymisierter Daten nicht möglich ist.

Selbstbestimmungsrechte werden komplett missachtet: Nach Art 33 Abs 5 soll in jenen Fällen, in denen nach nationalem Recht die Einwilligung der Betroffenen erforderlich ist, sich die Zugangsstelle für Gesundheitsdaten bei der Gewährung des Zugangs einfach „auf die in diesem Kapitel festgelegten Pflichten" berufen. Angesichts des grundsätzlichen Verarbeitungsverbotes von Gesundheitsdaten müssen Eingriffsnormen in das Grundrecht besonders präzise formuliert sein. Diese Anforderung erfüllt der Entwurf nicht. Informationsrechte für Betroffene nach der DSGVO werden einfach beseitigt, womit Betroffene von der Sekundärnutzung ihrer Daten in der Regel nichts erfahren und sich gegen mutmaßliche Rechtsverstöße auch nicht wehren können.

Die Aufsicht der unabhängigen Datenschutzbehörden (DSB) wird faktisch ausgeschaltet. Neue „Zugangsstellen für die Datennutzung" sollen die VO vollziehen und Datenzugriffe genehmigen. Ihr Aufsichtsziel ist, möglichst ungehinderten Datenzugriff EU-weit zu garantieren. Die Absicherung von Grundrechten zählt nicht dazu. Die Zugangsstellen sollen zwar mit den DSBs in vager Form „zusammenarbeiten". Deren Entscheidungskompetenz oder zumindest Mitwirkungsbefugnis an der Datengenehmigung ist aber überhaupt nicht abgesichert. Für das Vertrauen der Betroffenen in Vorhaben mit dieser grundrechtlichen Tragweite ist es wichtig, dass es eine starke und gut eingebundene Aufsicht gibt, die ihre Grundrechtsinteressen wahrnimmt.

Datengetriebene Forschung, Politiksteuerung und kommerzielle Innovationen stiften Nutzen, müssen aber grundrechtskonform sein. Die Interessen der Datenökonomie können und müssen auf für die Betroffenen schonendere Weise erfüllt werden. Die Nutzung ist auf anonymisierte, synthetische Daten oder solche, für die Zustimmungen der Betroffenen vorliegen, zu beschränken.

Verarbeitungserleichterungen nur bei sorgsam geprüften, wichtigen öffentlichen Gesundheitsinteresse. So könnte bei besonders sensiblen Kategorien an Daten grundsätzlich die Zustimmung jedes Einzelnen erforderlich sein. Weist der Datennutzer ein erhebliches öffentliches Interesse an seinem Forschungsgegenstand und seine fachliche Eignung nach, so könnte die Datenschutzbehörde die einzelnen Zustimmungen der Betroffenen durch ihre Genehmigung des Projektes ersetzen. Die Abwägung zwischen öffentlichen und individuellen Interessen sollte ein Gremium durchführen, dem Vertreter der Datenschutzbehörde, des Datennutzers und Dateninhabers und der Betroffenen angehören. Bei Daten und Zwecken, die keinen hohen Schutzgrad erfordern, ist denkbar, dass sie grundsätzlich weiterverarbeitet werden dürfen, es sei denn der Betroffene widerspricht nach eingehender Information über das Projekt.

Nennenswerte Sicherheit und Sanktionen fehlen: Ein derart zentralisierter Ansatz, der den Austausch von Daten aus unzähligen, voneinander getrennten sensiblen Anwendungen zum Ziel hat, entspricht aufgrund der leichten Angreifbarkeit weder dem Stand der Sicherheitstechnik noch bietet er ausreichend Gewähr, dass über die unterschiedlichsten Anwendungen hinweg keine hoch problematischen Personenprofile erstellt werden. Es sind Bestimmungen für eine Gefährdungshaftung/ Haftpflichtversicherung aufzunehmen, damit Betroffene leicht und ohne Klagseinbringung zu Schadenersatz gelangen, wenn ihre Daten entwendet bzw zweckwidrig genutzt werden.

Allgemeines zu den Zielen des Entwurfes:

- **Primärnutzung von Gesundheitsdaten:** Der Entwurf möchte die **„Kontinuität der Gesundheitsversorgung" bei Auslandsaufenthalten** verbessern. Reist jemand in andere Mitgliedsstaaten oder wechselt grenzüberschreitend den Wohnort, soll durch leichten elektronischen Zugriff auf Gesundheitsdaten auch die Versorgung und der Behandlungserfolg verbessert werden.

- **Patient:innen sollen raschen Zugriff auf ihre Daten erhalten**, die im Zuge von Gesundheitsdienstleistungen über ihre Person verarbeitet werden. Konkret wird das bestehende Auskunftsrecht der Datenschutz-Grundverordnung (DSGVO) in Bezug auf die Zeitkomponente erweitert. Jede/jeder soll „sofort in einem leicht lesbaren, gängigen und zugänglichen Format" auf eigene Daten zugreifen können. Die Bearbeitungsfrist von einem Monat nach der DSGVO entfällt.

- **Mit einem Binnenmarkt für Gesundheitsdaten sollen Gesundheitsdienste grenzüberschreitend einfacher erbracht werden können**. Die technische Infrastruktur für die Speicherung von Gesundheitsdaten ist weder zwischen noch innerhalb der Mitgliedsstaaten standardisiert und interoperabel. Generisch gewachsene Systeme müssten zunächst zusammengeführt werden.

- **Zentrales Motiv ist, der Datenökonomie ungehinderten Zugriff auf ihren Rohstoff für die Entwicklung neuer Produkte, Dienste**

und für Forschung bzw Politikgestaltung zu ermöglichen. An diesem Rohstoff hängen jedoch Grundrechte. Die Verwertung von Daten soll Vorrang vor den grundrechtlich geschützten Geheimhaltungsinteressen der Betroffenen erhalten. Jedes Unternehmen, jede Person oder Einrichtung, die bestimmte Sekundärnutzungszwecke verfolgt, soll EU-weit auf den riesigen Datenbestand zugreifen können. Dazu müssen alle „Dateninhaber" im „Gesundheits- und Pflegesektor" ihren Datenschatz personenbezogen an nationale „Zugangsstellen zu Gesundheitsdaten" herausgeben. Diese haben zunächst anonymisierte Daten anzubieten. Finden Datennutzer damit nicht das Auslangen (das dürfte der Regelfall sein, um zeitliche Verlaufsstudien anzufertigen), werden ohne Weiteres pseudonymisierte Daten bereitgestellt. Diese weisen einen (mittelbaren) Personenbezug auf, sind in hohem Maß schützenswert und unterliegen deshalb auch der Vollanwendung der DSGVO. Unverständlich dabei: Die Datenschutzbehörden spielen bei der Genehmigung der Datennutzung durch sogenannte Zugangsstellen zu Gesundheitsdaten keine Rolle. Dies wäre aber zur Absicherung der Grundrechte und einem angemessenen Interessensausgleich aus AK-Sicht zwingend nötig.

- **Freie Fahrt für die Datenökonomie:** Das bestimmende Motiv für die VO ist also die Einführung eines pauschalen Erlaubnistatbestandes für die Sekundärnutzung von Gesundheitsdaten. Die VO verdrängt die DSGVO, die die Zulässigkeit einer Weiterverarbeitung von vielen Abwägungen abhängig macht. Nach Art 6 Abs 4 DSGVO dürfen Daten nur für einen anderen Zweck, als jenem für den sie gesammelt wurden, genutzt werden, wenn dafür 1) eine Einwilligung der Betroffenen vorliegt, 2) ein Gesetz dies erlaubt und dies innerhalb einer Demokratie eine nötige wie verhältnismäßige Maßnahme ist oder 3) die Weiterverarbeitung mit dem ursprünglichen Sammelzweck – eng ausgelegt anhand der Erwartungen der Betroffenen – vereinbar ist.

- **VO geht der DSGVO unter Berufung auf überwiegende berechtigte Interessen vor:** Das Konzept der VO setzt sich über Art 6 Abs 4 DSGVO (strikt eingeschränkte Möglichkeiten der Sekundärnutzung) und Art 9 DSGVO (Verarbeitungsverbot von Gesundheitsdaten durchbrochen durch enge Ausnahmen) in praktisch jeder Hinsicht hinweg:
  - Zustimmungen der Betroffenen zur Weiterverarbeitung sind nicht vorgesehen.
  - Viele der nach der VO zulässigen Weiternutzungen sind mit dem Ursprungsweck nicht vereinbar und dürften aus Basis der DSGVO niemals weitergenutzt werden: Betroffene werden nicht damit rechnen (müssen) sondern überrascht sein, wo plötzlich überall ihre (pseudonymisierten) Daten auftauchen (Art 6 Abs 4 lit a und b DSGVO). Auch handelt es sich ausnahmslos um besonders schützenswerte Daten (Art 6 Abs 4 lit c).

- **Datengierige KI:** Die DSGVO gilt für die Künstliche Intelligenz (KI)-Forschung als Hemmschuh beim Akquirieren von Trainingsdaten. Über die Pflicht zur Datenbereitstellung durch sämtliche Gesundheits- und Pflegeberufe würden erstmals massenhafte Trainingsdaten für die Entwicklung von Künstlicher Intelligenz (KI) bereitstehen. Diese stünden bei Beachtung der DSGVO und ohne die pauschale Verarbeitungserlaubnis des vorliegenden Entwurfes keinesfalls in diesem Umfang zur Verfügung. Viele KI-Expert:innen sagen zudem: es braucht keine Daten von „echten" Personen. Synthetische, also künstlich erzeugte Daten, hinter der keine echte Person steht, verringern nicht die Ergebnisqualität, schützen aber echte Personen vor dem Missbrauch ihrer Daten.

- **Keine Schutzgarantien vor Missbrauch:** Schutzgarantien in Form von maximaler Datensicherheit und drakonische Sanktionen bei Sorgfaltsverstößen gibt es in der VO keine. Die Zugangsstellen zu den Gesundheitsdaten haften nur für den genehmigten, nicht aber für den missbräuchlichen Gebrauch. Präzise Anforderungen an den technischen Grad der Anonymisierung und Pseudonymisierung enthält die VO nicht. Eine Re-Identifizierung der Person ist daher nicht wirksam ausgeschlossen. Die einzige VO-Vorgabe: der Datennutzer darf niemanden re-identifizieren. Technischer Datenschutz, der sich nicht auf die Redlichkeit des Datennutzers verlässt, sondern den Rückschluss auf eine Person technisch unterbindet, ist nicht vorgesehen.

- **Rückschlüsse auf Personen möglich:** Die öffentlichen Zugangsstellen sollen offenbar Zugriff auf unmittelbar personenbezogene Daten haben, da sie konkrete Personen (und ihre behandelnden Ärzt:innen) verständigen dürfen, wenn eine Datenanalyse (von der die Betroffenen gar nichts wissen) zu einem Ergebnis kommt, das „Auswirkungen auf den Gesundheitszustand" der

Person hat. Pointiert dargestellte Folge: „Wie wir zu ihrer Person statistisch/ konkret erhoben haben, dürften Sie Träger eines Gendefektes sein, der unbehandelt ihre Lebenserwartung wahrscheinlich um X Jahre beschränkt." Zugangsstellen unterliegen nicht der Verschwiegenheitspflicht von Ärzt:innen und sollten keine Aufgaben erhalten, die einer vertrauensvollen Patient:innen-Ärzt:innen-Beziehung bedürfen.

- **Zweifel an der Grundrechtskonformität:** Gesundheitsdaten dürfen nach Art 9 DSGVO nur verarbeitet werden, wenn die betroffene Person ausdrücklich einwilligt, sie für die Gesundheitsvorsorge, Beurteilung der Arbeitsfähigkeit, Diagnostik, Behandlung oder die Gesundheitsverwaltung erforderlich sind oder die Verarbeitung gesetzlich vorgesehen ist. Auch lebenswichtige bzw erhebliche öffentliche Interessen, der Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards (bei der Gesundheitsversorgung, bei Arzneimitteln und Medizinprodukten) können die Verarbeitung von Daten rechtfertigen. Immer sind jedoch spezifische Rechtsgrundlagen und Maßnahmen „zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses erforderlich." Unionsrecht darf die Verarbeitung von Gesundheitsdaten nur vorsehen, wenn sie „in angemessenem Verhältnis zum verfolgten Ziel steht, den **Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht**, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich" ist.

  Dass diese Vorbehalte eingehalten werden, wird AK-seits bezweifelt: Mit Blick auf Umfang und Tiefe des Eingriffs in Grundrechte (Beschneidung der Transparenzrechte, keine Einwilligungs-/Widerspruchsrechte) beschneidet die pauschale Erlaubnis einer Sekundärnutzung personenbezogener Daten den Wesenskern des Datenschutzrechtes.

Bewertung im Detail:

Art 1 – Ziele

Nach Abs 4 bleibt die DSGVO unberührt. Die AK erachtet diese Aussage für unzutreffend. Die pauschalen Möglichkeiten für die Sekundärnutzung von personenbezogenen Gesundheitsdaten gehen über die Erlaubnistatbestände des Art 9 (Ausnahmen vom Verarbeitungsverbot von Gesundheitsdaten) und 89 DSGVO (Erleichterungen für Wissenschaft, Statistik und Forschung) weit hinaus.

AK-Anliegen: der Entwurf ist in Abstimmung mit dem EU-Datenschutzbeauftragten / Datenschutzausschuss DSGVO-konform zu überarbeiten.

Art 2 – Definitionen

Zu den **„elektronischen Gesundheitsdaten"** zählen nicht nur Daten „über die Gesundheit und genetische Daten" sondern auch Daten über „Gesundheitsfaktoren". Da so gut wie alle soziodemografischen Merkmale (insbesondere Wohn-, Bildungs-, Arbeits-, Herkunfts-, Familien-, oder Einkommensverhältnisse) bzw alle Aspekte von Lebensstilen, Vorlieben und Verhaltensweisen die Gesundheit beeinflussen können, eröffnet diese weitreichende Definition den Zugang zu praktisch allen Daten zu einer Person. Feingranulare Personenprofile werden dadurch ermöglicht.

AK-Anliegen: Eine wichtige Stellschraube für einen grundrechtskonformen Datenzugriff wäre eine beschränkende Präzisierung der erfassten Daten.

„Wellness-Anwendungen" sind Geräte oder Software, die von Konsument:innen für andere Zwecke als der Gesundheitsversorgung verwendet werden, etwa „zur Erzeugung von Wohlbefinden und zur Einhaltung eines gesunden Lebensstils."

AK-Anliegen: Da Konsument:innen weder damit rechnen, noch damit rechnen müssen, dass diese Daten über eine zentrale Abrufstelle für alles Mögliche verwertet werden und überdies oft auch eine zweifelhafte Datenqualität aufweisen, besteht für ihre Einbeziehung in den Entwurf kein Anlass. Die Definition sollte ersatzlos gestrichen werden.

Art 10 Digitale Gesundheitsbehörde

Sie ist ua für die Umsetzung der Kapitel II und III zuständig. In einem jährlichen Tätigkeitsbericht muss sie lediglich über die Zusammenarbeit mit den für Datenschutz, Cybersicherheit und künstliche Intelligenz zuständigen Stellen informieren.

AK-Anliegen: Die Behörde sollte sich durch gesetzliche Bestimmungen die Aufgaben recht sicher mit der Datenschutzbehörde (DSB) teilen.

Art 12 – MyHealth@EU

Diese von der Kommission eingerichtete Plattform soll den Datenaustausch zwischen den nationalen Kontaktstellen für die digitale Gesundheit erleichtern. Alle Gesundheitsdienstleister müssen mit nationalen Kontaktstellen für die digitale Gesundheit verbunden sein, Daten austauschen und sind gemeinsam datenschutzrechtliche Verantwortliche für die Daten auf der MyHealth-Plattform. Auch Verschreibungen, die via der MyHealth-Plattform zugänglich sind, müssen grenzüberschreitend in herkömmlichen und Online-Apotheken einlösbar sein. Delegierte Rechtsakte der Kommission sollen „die Sicherheit, Vertraulichkeit und den Schutz elektronischer Gesundheitsdaten" gewährleisten. Die Zuständigkeiten aller Beteiligten legt die Kommission in delegierten Akten fest.

AK-Anliegen: Sicherheitsmaßnahmen müssen ein Kernbereich des Vorhabens sein, zumal die zentralisierte Datenspeicherung und EU-weite Datentransfers in dieser Größenordnung besonders missbrauchsgeneigt und bevorzugtes Ziel für kriminelle Angreifer sein dürfte. Vor diesem Hintergrund sind auch besondere Haftungsbestimmungen aufzunehmen, damit Betroffene leicht und ohne eine Klage einbringen zu müssen zu Schadenersatzzahlungen gelangen, wenn ihre Daten entwendet bzw zweckwidrig genutzt werden. Bezüglich der Kritik an delegierten Akten wird auf Art 5 verwiesen.

Art 14 – Zusammenspiel mit Bestimmungen zu Medizinprodukten und KI

Wer Medizinprodukte oder hochriskante KI (künstliche Intelligenz) herstellt, die mit elektronischen Patient:innenakten interoperabel sind, muss auch die VO-Vorschriften zur Interoperabilität einhalten. Bestehende Vorschriften „für die Beschaffung, Erstattung, Finanzierung" von elektronischen Patient:innenakt-Systemen können beibehalten werden.

AK-Anliegen: Von hochriskanter KI gehen – worauf der Name bereits hinweist – schwer kalkulierbare und beherrschbare Risiken aus. Vor diesem Hintergrund wäre es nicht angemessen, über interoperable elektronische Patient:innenakten-Systeme Datenanalysen aus hochriskanter KI ohne Weiteres über eine EU-weite Infrastruktur zu teilen. Die Folgen bias-behafteter Ergebnisse und falscher Schlussfolgerungen könnten im Gesundheitsbereich fatal sein.

Art 33 – Mindestkategorien an Daten für die Sekundärnutzung

Jeder Dateninhaber hat die sensibelsten Daten zur Verfügung zu stellen und das in einem erheblichen Ausmaß: Daten aus Patient:innenakten, zu „gesundheitsrelevanten Faktoren, einschließlich sozialer, umweltbedingter und verhaltensbezogener Gesundheitsfaktoren wie Versicherungsstatus, beruflicher Status, Bildung, Lebensstil, Wohlbefinden und Verhaltensdaten" , Gen- bzw Genom-Daten, Daten vom „Internet der Dinge" wie Fitness-Tracker und Wellness-Apps, aus den Medizin-Registern öffentlicher Stellen, aus klinischen Prüfungen und „Anreicherungen" mit anderen Daten. Zu den zur Datenweitergabe verpflichteten Dateninhabern zählen der öffentliche wie private Gesundheits- und Pflegesektor, Forschungs- und EU-Einrichtungen.

Abs 5 normiert: „Ist nach nationalem Recht die Einwilligung der natürlichen Person erforderlich, so berufen sich die Zugangsstellen für Gesundheitsdaten bei der Zugangsgewährung auf die in diesem Kapitel festgelegten Pflichten." In Notsituationen (entsprechend der vagen Definition im Entwurf zu einem EU-Datengesetz, das AK-seits ebenfalls heftig kritisiert wurde) sollen die Gesundheitsdaten nach Abs 6 auch noch mit ganz anderen Daten zusammengeführt werden dürfen.

AK-Anliegen: Aufgrund der Eingriffstiefe in Grundrechte wird diese Bestimmung vehement abgelehnt. Nicht nur werden die Datenarten und Herausgabepflichtigen nicht so präzise festgelegt, dass von einer ausreichend determinierten Eingriffsnorm die Rede sein kann. Auch der angestrebte Datenumfang ist unverhältnismäßig: alle nur denkbaren Verhaltensdaten könnten herausverlangt und mittelbar personenbezogen ausgewertet werden. Die Weitergabe-Pflichten des Art 33 scheinen pauschal dem datenschutzrechtlichen Zustimmungsrecht vorzugehen. Das ist inakzeptabel. Die Bestimmung ist ebenso ersatzlos zu streichen wie Abs 6, der eine Blankoermächtigung für den Abgleich mit anderen Daten in völlig unspezifischen „Notsituationen" vorsieht.

Art 34 – Sekundärnutzungszwecke

Zu den Weiterverarbeitungszwecken zählen „Tätigkeiten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit und am Arbeitsplatz, Unterstützung der Aufgaben von öffentlichen und EU-Stellen, Bildungs- und Lehrtätigkeiten, Forschung, Training von Algorithmen und KI-Systemen, die zur öffentlichen Gesundheit, sozialen Sicherheit oder personalisierten Gesundheitsversorgung beitragen".

Abs 3 ordnet an, dass nach dem Entwurf zu einem Datengesetz auch „Zugang zu in privatem Besitz befindlichen Daten gewähreistet“ wird, „um einem öffentlichen Notstand“ vorzubeugen…“.

AK-Anliegen: Die Zweckbeschreibungen sind viel zu vage und unbestimmt und stellen damit keine taugliche Rechtsgrundlage für den Eingriff in die Datenschutzrechte und Privatsphäre der Betroffenen dar. Das Zugangsrecht zu wie immer gearteten „privaten Daten“ im Notfall ist derart unbestimmt und überschießend, dass auch nur eine ersatzlose Streichung in Frage kommt.

Art 35 – Unerlaubte Sekundärnutzung

Dass das vorliegende Konzept grundrechtlich unbedenklich und risikofrei ist, glaubt die Kommission selbst nicht. Anders kann die vorliegende Bestimmung nicht interpretiert werden. Sie verbietet das „Treffen von Entscheidungen zum Schaden einer natürlichen Person auf der Grundlage ihrer Gesundheitsdaten“ etwa dadurch, dass Konsument:innen von Versicherungsverträgen ausgeschlossen oder Prämien erhöht werden. Ua ist die auf Konsument:innen abzielende Werbung und Vermarktung verboten und die Entwicklung von Produkten und Diensten, die Personen und der Gesellschaft schaden können.

AK-Anliegen: Wenn kein Rückschluss auf die betroffene Person bei der Weiterverarbeitung ihrer pseudonymisierten Daten möglich wäre, bedürfte es keines Hinweises, dass niemand durch auf seinen Daten basierende Entscheidungen geschädigt werden darf. In dieselbe Richtung zielt das Verbot, dass durch die Datenweiterverarbeitung niemand von Versicherungsverträgen ausgeschlossen oder die Prämie geändert werden darf. Es wird augenscheinlich damit gerechnet, dass Auswertungen – unerlaubterweise – doch personenbezogen sein können und nicht zum öffentlichen Wohl beitragen. Angesichts des beschriebenen Risikopotentials ist es unakzeptabel, dass den Betroffenen bei der Datennutzung jede Selbstbestimmung abgesprochen wird.

Art 36 und 37 – Zugangsstellen für Gesundheitsdaten

Die Stellen sind weisungsunabhängig und arbeiten „aktiv mit Vertretern der Interessensträger, vor allem der Patienten, Dateninhabern und -nutzern zusammen”.

AK-Anliegen: Trotz der immensen Grundrechtssensibilität des Vorhabens wird unverständlicherweise die Zusammenarbeit mit den Datenschutzbehörden (DSB) nur kursorisch erwähnt: Die Zugangsstelle für Gesundheitsdaten möge mit ihnen zusammenarbeiten und über Sanktionen bei Datenmissbrauch nach Art 43 verständigen. Nötig wäre eine Vorabprüfung der Datenschutzkonformität jedes Projektes durch die DSB, bevor die Zugangsstelle ein Genehmigungs-verfahren in Gang bringt. Auch die Art der Zusammenarbeit mit anderen Stakeholdern bleibt unbestimmt. Patient:innenvertretungen erhalten va keinerlei verbriefte Rechte.

Art 38 – Pflichten der Zugangsstellen gegenüber Konsument:innen/Patient:innen

Die Zugangsstellen sind nicht verpflichtet, jeder Person die Informationen nach Art 14 DSGVO über die Nutzung ihrer Daten zu geben. Es reicht, dass allgemeine Informationen über alle erteilten Genehmigungen veröffentlicht werden. Mit anderen Worten: der/die Betroffene erfährt nicht, ob, von wem, wofür und in welchem Umfang seine Daten genutzt werden. Damit tappen Betroffene im Dunkeln, an wen sie Auskunftsbegehren nach der DSGVO richten und wie sie die Rechtmäßigkeit der Verarbeitung prüfen können.

Erhält die Zugangstelle vom Datennutzer einen Befund, der sich auf die Gesundheit einer bestimmten Person auswirken kann, so kann die Zugangsstelle die Person (und ihre behandelnden Ärzt:innen) darüber unterrichten.

AK-Anliegen: Die Rechte der Betroffenen werden unvertretbar ausgehöhlt. Transparenz über die Verarbeitung ist ein Kernelement des Grundrechts auf Datenschutz. Dass die in der DSGVO enthaltenen, individuellen Informationspflichten der Datenverarbeiter entfallen, ist inakzeptabel. Jede Form von Rechtsschutz setzt die Kenntnis der Verarbeitung persönlicher Daten voraus.

Art 43 – Sanktionen der Zugangsstellen

Die Stellen haben Dateninhaber und –nutzer zu überwachen. Sie haben Geldbußen zu verhängen, wenn Dateninhaber die Datennutzung behindern oder verzögern.

AK-Anliegen: Es ist ausdrücklich vorzusehen, dass den DSB bezüglich der DSGVO-Konformität eine Vorabgenehmigungs- und Überwachungspflicht bei der Durchführung einer auf personenbezogenen Daten basierenden Analyse zukommt. Die Sanktionierung der Dateninhaber ist äußerst problematisch, da der Grund für eine Zugangsbeschränkung auch Zweifel an der Rechtskonformität des Datenzugangs sein können. Dateninhaber (va Ärzt:innen, Krankenhauspersonal) sind auch ihren Patient:innen gegenüber zu Vertraulichkeit verpflichtet.

Art 44 – Datenminimierung, Zweckbegrenzung

Die Zugangsstelle stellt zunächst anonymisierte Daten zur Verfügung. Kann der Verarbeitungszweck damit nicht erreicht werden, werden die Daten pseudonymisiert bereitgestellt. Datennutzer stellen „die Identität der pseudonymisierten Daten" nicht wieder her – sofern doch, werden „angemessene Sanktionen" verhängt.

AK-Anliegen: Da Entwicklungen einer Person gerne im Zeitverlauf erhoben und dargestellt werden, reichen anonymisierte Daten oft nicht aus. Ganz entschieden abzulehnen ist, dass die Pflicht eine Re-Identifizierung zu unterlassen, bloß an den Datennutzer gerichtet ist. Dieser kann sorgfaltswidrig oder von Beginn an unredlich vorgehen. Konsument:innen und Patient:innen dürfen diesem Risiko niemals ausgesetzt werden. Aus AK-Sicht ist es die Pflicht der Zugangsstelle, Daten derart zu anonymisieren bzw pseudonymisieren, dass eine Re-Identifikation so gut wie ausgeschlossen ist. Siehe diesbezüglich die Unterscheidung zwischen technischer, faktischer und absoluter Anonymität.

Art 46 – Datengenehmigung

Die Zugangsstellen prüfen, ob der Antrag den Zwecken dient, die die VO auflistet, die Daten erforderlich sind und der Antragsteller den Anforderungen der VO entspricht. Nach erteilter Genehmigung, die bis zu 5 Jahren gilt und verlängert werden kann, fordert die Zugangsstelle die Daten unverzüglich beim Dateninhaber an. Die Datennutzer veröffentlichen spätestens nach 18 Monaten anonymisierte Ergebnisse „einschließlich der für die Gesundheitsversorgung relevanten Informationen". Sie unterrichten die Zugangsstelle nach Abs 12 auch „über alle klinisch signifikanten Befunde, die Folgen für den Gesundheitszustand der natürlichen Person haben können, deren Daten im Datensatz enthalten sind." Nach Abs 14 ist die Haftung der Zugangsstelle „auf den Umfang der erteilten Datengenehmigung bis zur Beendigung der Verarbeitung begrenzt."

AK-Anliegen: Die DSB ist zwingend in den Genehmigungsprozess miteinzubeziehen. Sie hat ua etwa zu prüfen, ob von den Betroffenen Einwilligungen/Widersprüche nach der DSGVO vorliegen oder ein derart wichtiges öffentliches Interesse an der konkreten Datenauswertung besteht, dass eine Genehmigung der DSB die Einzelzustimmungen der Betroffenen ersetzen kann. Außerdem erteilt sie Auflagen, damit etwa die Datensicherheit gewährleistet ist. Abs 12 betrifft höchstpersönliche Entscheidungen jeder/s Einzelnen, wem er/sie etwas anvertraut und damit auch das Ärztegeheimnis: ohne vorherige Zustimmung des/der Betroffenen zum Projekt würde sich Abs 12 unvertretbar auf die Persönlichkeitsrechte auswirken. Die Haftung der Zugangsstelle sollte als verschuldensunabhängige Gefährdungshaftung ausgestaltet sein und unbedingt auch zweckwidrige, missbräuchliche Weiterverwendungen umfassen. Bei Missbrauch durch den Datennutzer hat sie Betroffene ebenfalls zu entschädigen und kann anschließend gegenüber dem Rechtsverletzer Regress üben.

Art 50 – sichere Verarbeitungsumgebung

Die Zugangsstellen minimieren Missbrauchsrisiken durch „modernste" technische Mittel. Die Datennutzer können nur Daten, die nicht personenbezogen sind, aus der sicheren Verarbeitungsumgebung herunterladen.

AK-Anliegen: Die Vorgaben sind unklar und sogar widersprüchlich. Die Nutzer dürfen nur anonymisierte Ergebnisse veröffentlichen. Diese Pflicht ist sinnentleert, wenn diese ohnehin nur „nicht personenbezogene" Daten herunterladen können. Datennutzer dürfen nach Art 44 die Identität hinter den pseudonymisierten Daten nicht wieder herstellen. Auch dies müsste ausgeschlossen sein, wenn ohnehin nur vollständig anonymisierte Daten herunterladbar sind.

Kontaktieren Sie uns!

In Wien:

Daniela Zimmer
daniela.zimmer@akwien.at

In Brüssel:

Alice Wagner
alice.wagner@akeuropa.eu

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Wien, Österreich
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

AK EUROPA
Ständige Vertretung Österreichs bei der EU
Avenue de Cortenbergh 30
1040 Brüssel, Belgien
T +32 (0) 2 230 62 54

www.akeuropa.eu

Über uns

Die Bundesarbeitskammer (AK) ist die gesetzliche Interessenvertretung von rund 3,8 Millionen Arbeitnehmer:innen und Konsument:innen in Österreich. Sie vertritt ihre Mitglieder in allen sozial-, bildungs-, wirtschafts- und verbraucherpolitischen Angelegenheiten auf nationaler sowie auch auf der Brüsseler EU-Ebene. Darüber hinaus ist die Bundesarbeitskammer Teil der österreichischen Sozialpartnerschaft. Die AK ist im EU-Transparenzregister unter der Nummer 23869471911-54 registriert.

Die Aufgaben des 1991 eröffneten AK EUROPA Büros in Brüssel sind einerseits die Repräsentation der AK gegenüber europäischen Institutionen und Interessensorganisationen, das Monitoring von EU-Aktivitäten und die Wissensweitergabe von Brüssel nach Österreich, sowie gemeinsam mit den Länderkammern erarbeitete Expertise und Standpunkte der Arbeiterkammer in Brüssel zu lobbyieren.