19. April 2021

ver.di-Stellungnahme

zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz / Data Governance Act, DGA)

COM(2020) 767 final, 2020/0340 (COD) vom 25. November 2020

Abstract:

Mit ihrem Vorschlag für eine Verordnung über europäische Daten-Governance (DGA) beabsichtigt die Europäische Kommission, die Verarbeitung von (sensiblen) Daten unter Beachtung der europäischen Grundwerte zu erleichtern.

ver.di begrüßt grundsätzlich, dass *nicht-personenbeziehbare* Daten zur Stärkung des Gemeinwohls und des Europäischen Binnenmarktes verfügbar gemacht sowie Wege für innovative gemeinwohlorientierte Datentreuhänderschaften geebnet werden sollen.

ver.di steht jedoch der Weitergabe und externen Weiterverarbeitung von explizit sensiblen Daten der europäischen öffentlichen Daseinsvorsorge insoweit kritisch gegenüber, als dass dadurch

- das Vertrauen der Bürger*innen in die Erhebung und Verarbeitung von Daten durch die öffentliche Verwaltung geschwächt werden könnte,
- die Gefahr von Datenmissbrauch erhöht werden könnte,
- der Beschäftigtendatenschutz und die Persönlichkeitsrechte der Bürger*innen nicht ausreichend gewahrt werden könnten,
- die Konzentrierung von datenbasierter Macht, sei sie politischer oder wirtschaftlicher Art, verstärkt und der europäische Binnenmarkt dadurch sogar geschwächt werden könnte, und
- die öffentliche Daseinsvorsorge unter Privatisierungsdruck geraten könnte.

Kritisch sieht ver.di weiterhin:

- dass bei der Datenerschließung nicht Daten des privaten Sektors im Fokus stehen, sondern die (sensiblen) Daten des öffentlichen Sektors, und
- dass im Gesetzentwurf die Bedeutsamkeit des öffentlichen Dienstes bei der gemeinwohlorientierten Nutzung und Aufbereitung von Daten unterbelichtet ist.

Entscheidend ist aus ver.di-Sicht daher, dass der Vorschlag grundsätzlich überarbeitet wird, um die oben genannten Risiken auszuschließen und ihm eine klare gemeinwohl- und grundrechtsorientierte Ausrichtung zu geben. Dazu gehört, die digitale Souveränität von der lokalen bis zur europäischen Ebene sowie den europäischen Binnenmarkt zu stärken und Datenmonopolen entgegenzuwirken.

Die Nutzung von Daten für das Gemeinwohl und die Stärkung insbesondere der europäischen Wirtschaft sind wünschens- und unterstützenswerte Ziele. Die Strategien, um diese Zielsetzungen zu erlangen, müssen im Einklang mit europäischen Grundrechten stehen und sollten Demokratie und Freiheit möglichst stärken, keinesfalls aber schwächen. Das bedeutet, Persönlichkeitsrechte der Bürger*innen zu wahren, ihre informationelle Selbstbestimmung zu gewährleisten und einen Kernbereich der Persönlichkeitsrechte von der Handelbarkeit auszunehmen sowie die digitale Daseinsvorsorge und europäische Wirtschaft zu stärken und Monopolbildungen entgegenzuwirken.

Inwieweit der vorliegende Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) diese Anliegen erfüllt, wird im Folgenden erörtert.

Regelungsbestandteile des Daten-Governance-Gesetzes sollen unter anderem sein:

- *Die kommerzielle Weiternutzung von Daten des öffentlichen Sektors, die bisher explizit aufgrund der Gesetze zu Datenschutz, Urheberrecht und Geschäftsgeheimnissen vor dem Zugriff Dritter geschützt sind,*
- *Anmelderegelungen für Unternehmen und Organisationen, die Daten gemeinsam nutzen wollen, für Datenvermittler (Datenintermediäre), die als Treuhänder zwischen Privatpersonen und Datennutzern zwischengeschaltet sind und für Organisationen, die „gespendete" Daten zum Wohl der Allgemeinheit sammeln.*

Der Verordnungsentwurf soll die Richtlinie (EU) 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtlinie) ergänzen. Diese enthält bereits einen Rechtsrahmen für die kommerzielle und nichtkommerzielle Verwertung von Daten der öffentlichen Hand – allerdings mit der wesentlichen Einschränkung, dass Rechte Dritter der Weiterverwendung nicht entgegenstehen dürfen. Zugleich wird in Art. 3 Abs. 3 des Kommissionsvorschlags festgehalten, dass öffentliche Stellen durch den DGA nicht von ihren Geheimhaltungspflichten und den bestehenden Datenschutzbestimmungen befreit sind.

Eine mögliche Weitergabe von Daten hängt zentral von der technischen und organisatorischen Umsetzung, den rechtlichen Kontroll- und Sanktionsmöglichkeiten sowie einer Einstufung der Daten in Kritikalitätsstufen ab. Zu berücksichtigen ist dabei auch, dass viele Daten, wie zum Beispiel personenbeziehbare aus dem Gesundheits-, Finanz- und Mobilitätsbereich derart sensibel sind, dass eine Weitergabe schon aus Sicherheitsgründen zu unterbinden ist. Einzukalkulieren bei einer Weitergabe von Daten und Einrichtung von „Datenpools" ist, dass dadurch attraktive Ziele für Hackerangriffe (seien sie politisch oder finanziell motiviert) kreiert werden, womit ein hohes Sicherheitsniveau mit hohen Kosten für Technik und Personal einhergeht und dennoch keine absolute Sicherheit garantiert werden kann. Deshalb ist es wichtig, von vornherein demokratie- und sicherheitsrelevante Daten, die zum „Profiling" und „Scoring" von Bürger*innen genutzt werden können oder die Rückschlüsse auf die Vulnerabilität (Verwundbarkeit) der öffentlichen Grundversorgung zulassen, kategorisch von der Weitergabe auszuschließen. Bereits die Erhebung und Speicherung solcher Daten im öffentlichen Sektor ist grundsätzlich kritisch zu sehen.

Der Wunsch nach einer ungehinderten Datenökonomie unter grundrechtlich abgesicherten Bedingungen kann nicht vollständig verwirklicht werden. Hier sollte an konfligierenden Stellen ein klares Bekenntnis zu den Grundrechten gegeben werden. Instrumente zur Gewährleistung der Datensicherheit müssen eindeutig und wirksam sein. Im vorliegenden Gesetzesentwurf ist die Förderung der Datenbewirtschaftung sehr klar formuliert; die flankierenden Maßnahmen und Vorschriften, die die Rechte der Betroffenen absichern sollen, sind es nicht im gebotenen Maße.

Erstaunlich ist, dass im vorliegenden Gesetzesentwurf kontinuierlich über die Bereitstellung von Daten des europäischen öffentlichen Sektors für den europäischen Binnenmarkt die Rede ist, die Daten jedoch weltweit zugänglich gemacht werden sollen. Es wird nicht darauf eingegangen, wie vermieden werden soll, dass durch die verbesserte Datenverfügbarkeit bestehende Monopol- bzw. Oligopol-Stellungen außereuropäischer Unternehmen gestärkt werden.

Gute Rahmenbedingungen für innovative öffentliche Infrastrukturen sind für das datenbasierte Gemeinwohl essenziell. Im Gesetzesentwurf wird jedoch nicht auf die wichtige Funktion des öffentlichen Dienstes eingegangen, der dringend technisch und personell in die Lage versetzt werden sollte, selbst die Daten des öffentlichen Sektors für das Gemeinwohl zu verwerten und nutzbar zu machen. Vielmehr werden Kosten, die der öffentlichen Hand durch eine möglichst sichere Weitergabe von Daten entstehen, im DGA-Entwurf eher kleingerechnet.

ver.di hält folgende Punkte und Änderungen für die Überarbeitung und Neuausrichtung des Daten-Governance-Gesetzes (DGA) für wesentlich.

Umfassende Geltung der Datenschutzgrundverordnung: Dass die Europäische Kommission sich weiterhin klar zur Datenschutzgrundverordnung (DSGVO) bekennt, ist richtig. Insofern sollte auch gleich in Artikel 1 deutlich gemacht werden, dass die DSGVO weiterhin voll umfänglich gilt. Bei jedem Regelungsvorschlag bedarf es einer Prüfung, ob dieser im Einklang mit der DSGVO umgesetzt werden kann.

Keine Weiterverwendung von Beschäftigtendaten: Die Weiterverwendung von Beschäftigtendaten muss ausgeschlossen werden. Es ist zu prüfen, ob Daten der öffentlichen Daseinsvorsorge auch Beschäftigtendaten enthalten, zum Beispiel im Bereich der Mobilität.

Keine Schwächung des europäischen Binnenmarktes und keine Stärkung vorhandener Datenmonopole: Es müssen Maßnahmen aufgezeigt werden, mittels derer vermieden werden kann, dass infolge einer allgemeinen weltweiten Bereitstellung (sensibler) europäischer Daten der Daseinsvorsorge der europäische Binnenmarkt geschwächt und bestehende Monopol- bzw. Oligopol-Stellungen diverser Daten-Unternehmen (die vor allem im außereuropäischen Raum zu finden sind) gestärkt werden. Dies könnte beispielsweise mit Auflagen zur Nutzung offener technischer Standards und Schnittstellen sowie zur europäischen Speicherung und Verarbeitung von Daten erreicht werden.

Stärkung der digitalen Souveränität und Daseinsvorsorge von der lokalen bis zur europäischen Ebene: Es müssen Maßnahmen aufgezeigt werden, mittels derer vermieden werden kann, dass durch die weltweite Bereitstellung (sensibler) europäischer Daten der Daseinsvorsorge diese nicht selbst gefährdet wird und unter Privatisierungsdruck gerät. Bei der Definition von Rahmenbedingungen zur Daten-Governance muss gewährleistet sein, dass einerseits die Relevanz öffentlicher Infrastrukturen für ein datenbasiertes Gemeinwohl berücksichtigt wird und andererseits die digitale Souveränität von der lokalen bis zur europäischen Ebene gefördert wird.

Begriffsunklarheiten beseitigen: Zentrale Begriffe wie „Dienste für die gemeinsame Datennutzung“ und „Zwecke in allgemeinem Interesse“ sollten klarer als bisher in Artikel 2 definiert werden.

Klare Trennung personenbezogener von nicht-personenbezogenen Daten vonnöten: Problematisch ist, dass der DGA-Vorschlag nicht deutlich genug zwischen Daten unterscheidet, die personenbeziehbar und solchen, die nicht-personenbeziehbar sind (und ob es sich um besonders schützenswerte sensible Daten handelt). Ob Schutzmaßnahmen ausreichen, hängt jedoch entscheidend von der Kategorie der Daten ab. Dieses Defizit kann zu Rechtsunsicherheiten führen.

Der grundrechtliche Schutz personenbezogener und -beziehbarer Daten darf nicht untergraben werden.

Umkehr des Begründungszwangs der Verarbeitung personenbezogener Daten: Die in Art. 3 Abs. 1 lit. a-c aufgeführten drei Datenkategorien (geschäftliche und statistische Geheimhaltung und Schutz geistigen Eigentums Dritter) unterscheiden sich maßgeblich von der vierten, dem „Schutz personenbezogener Daten". Nach Datenschutzrecht muss jede Verarbeitung personenbezogener Daten erlaubt sein. Auch wenn öffentliche Stellen nicht gezwungen sind, Daten für Unternehmen und anderen Akteur*innen zur Verfügung zu stellen, werden sie künftig unter Druck stehen, zu begründen, warum sie dies nicht tun bzw. warum sie gewisse Schutzmaßnahmen treffen.

Streichung der Datenkategorie „Schutz personenbezogener Daten": Die DSGVO gilt in vollem Umfang. Im Kapitel II des vorliegenden Gesetzentwurfs werden in Bezug auf personenbeziehbare Daten keine Regelungen geschaffen, die nicht bereits von der DSGVO abgedeckt wären. Insofern ist die in Art. 3 Abs. 1 lit. d genannte vierte Datenkategorie „Schutz personenbezogener Daten" aus dem Katalog der dort gelisteten Kategorien zu streichen. Die Beibehaltung dieser Kategorie würde nur zu Verwirrung und Rechtsunsicherheit führen.

Für Datentransfers braucht es konkrete Datensicherungsmaßnahmen: Der Kommissionsvorschlag enthält in Art. 5 Abs. 4 keine Regelungen zu ausreichenden technischen und organisatorischen Maßnahmen für den sicheren Datentransfer zwischen öffentlichen Stellen und Unternehmen. Dabei geht es um Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung von personenbezogenen Daten sowie deren Weitergabe.

Bestehende Anonymisierungstools unzureichend: Techniken der De-Personalisierung, die in Teilen erlaubt sein könnten, sind noch nicht ausreichend entwickelt. Bisher sind die Risiken der Re-Personalisierung zu hoch. Die Forschung für wirksame Anonymisierungstools sollte gestärkt werden. Es erschließt sich nicht, warum die Thematisierung des Risikos einer Re-Identifizierung betroffener Personen anhand anonymisierter Daten, wie sie in Art 5 Abs. 11 behandelt wird, sich ausschließlich auf Datenübertragungen in Drittländer bezieht. Vorkehrungen und Beschränkungen gegen eine rechtswidrige Aufhebung der Anonymisierung müssen selbstverständlich auch für Daten, die in der EU zirkulieren, getroffen werden. Wünschenswert wäre zudem eine Ergänzung um die strukturelle Förderung der Forschung von Techniken, die „privacy by design" verwirklichen und somit dazu beitragen, nicht nur spätere Konflikte und Vertrauensverluste zu vermeiden, sondern es vereinfachen würden, Daten direkt als „Open Data" zur Verfügung zu stellen.

Unternehmen dürfen keinen Direktzugriff auf geschützte Daten erhalten: Laut Art. 5 Abs. 3 des Kommissionsvorschlag können öffentliche Stellen die Verpflichtung auferlegen, dass nur anonymisierte oder pseudonymisierte Daten weiterverwendet werden dürfen oder vertrauliche Geschäftsinformationen gelöscht werden sollen. Wer die Anonymisierung bzw. Pseudonymisierung vornimmt, ist nicht ausdrücklich geregelt. Deshalb muss geregelt werden, dass ein Direktzugriff von Unternehmen auf geschützte Daten zur eigenständigen Anonymisierung bzw. Pseudonymisierung nicht stattfindet.

Es bedarf klarer Regeln für die Anonymisierung und Pseudonymisierung personenbezogener Daten: Im Kommissionsvorschlag bleibt unklar, wann Daten als anonymisiert bzw. pseudonymisiert gelten und wer für die Anonymisierung bzw. Pseudonymisierung verantwortlich ist. Aufgrund der technischen Weiterentwicklung durch Big Data und Künstlicher Intelligenz kann nicht mehr eindeutig bestimmt werden, ob Daten einen Personenbezug aufweisen oder nicht. Daher muss einerseits festgelegt werden, welche Kategorie Daten niemals, d. h. weder anonymisiert noch pseudonymisiert, verwendet werden dürfen, und andererseits, ab wann Daten als hinreichend bzw. vollständig anonymisiert gelten, damit diesbezüglich Rechtssicherheit für die Betroffenen geschaffen

wird. Der derzeitige Stand der Technik ist für Maßnahmen zur Anonymisierung noch unzureichend. Für pseudonymisierte Daten – also personenbezogene Daten, die mit zusätzlichen Informationen wieder repersonalisiert werden können – sollte geregelt werden, dass entweder die betroffene Person selbst (z. B. freigewählte NutzerID) oder eine Zertifizierungsstelle oder Datentreuhänder der*dem Betroffenen das Pseudonym zuweist und verwaltet.

Cloud-Dienste dürfen nicht zur Speicherung von personenbezogenen Daten genutzt werden: Die Nutzung von Cloud-Diensten zur Speicherung von Daten ist datenschutzrechtlich bedenklich, weil bisher nur unzureichend sichergestellt ist, dass sich die genutzten Speicher in der EU befinden und die Anforderungen an den Datenschutz umfassend erfüllen. Außerdem ziehen die Daten in der Cloud häufig um, werden also von Speicherort zu Speicherort transferiert. Daher ist es begrüßenswert, dass sich die Verordnung gemäß Erw. 22 des Kommissionsvorschlags nicht auf Anbieter von Cloud-Diensten erstrecken soll. Es ist darauf zu achten, dass dies so bleibt.

Perspektivische Anonymisierungspflicht vor der Datenweitergabe: Öffentliche Stellen müssen, wenn die Anonymisierungstechnologien fortentwickelt und qualitativ ausreichend sein sollten, ausdrücklich einer Pflicht unterliegen, Daten zu anonymisieren bevor sie Daten (ohne Zustimmung Betroffener) weitergeben. Nach dem derzeitigen technischen Stand ist die Anonymisierung unzureichend. Es sind Vorgaben vorzusehen, wann Daten als verlässlich anonymisiert gelten.

Wettbewerbsfähigkeit darf kein Gradmesser für die Weiterverwendung von Daten sein: Laut Art. 5 Abs. 2 des Kommissionsvorschlags sollen die Bedingungen für die Weiterverwendung von Daten im Besitz öffentlicher Stellen nichtdiskriminierend, verhältnismäßig und objektiv sein und dürfen nicht der Behinderung des Wettbewerbs dienen. Diese Bedingungen sind ungenau und bieten demzufolge keine Rechtssicherheit.

Öffentliche Stellen dürfen nicht zur Weitergabe von Daten verpflichtet werden. Der Kommissionsvorschlag sieht laut Art. 3 Abs. 3 vor, dass öffentliche Stellen nicht dazu verpflichtet werden können, die Weiterverwendung von Daten zu erlauben. Zudem räumt er es laut Art. 6 Abs. 1 den öffentlichen Stellen ein, Gebühren für die Erlaubnis der Weiterverwendung von Daten erheben zu dürfen. Beides ist ausdrücklich begrüßenswert und muss beibehalten werden. Die Möglichkeit Gebühren zu erheben, darf jedoch kein Anreizprinzip zum Verkauf (und der Absenkung des Schutzes) sensibler Daten bilden.

Stärkung der für Datenschutz und Datensicherheit zuständigen Behörden: Zur Gewährleistung von Datenschutz und Datensicherheit müssen die zuständigen Behörden und Einrichtungen personell, technisch und finanziell adäquat ausgestattet werden.

Regelungsrahmen für Datenintermediäre ist begrüßenswert: Dass mit dem DGA ein Regelungsrahmen geschaffen werden soll, der das Vertrauen in Datenintermediäre stärkt, ist positiv und ausdrücklich begrüßenswert. Jedoch bedarf es dazu weiterer Maßnahmen, als bisher im Kommissionsvorschlag vorgegeben. Nur wenn die Rechte der Bürger*innen gewahrt werden, ist ihr Vertrauen begründet.

Obligatorisches Zertifizierungssystem für Datenintermediäre: Sowohl um die Risiken zu begrenzen, die mit der zentralen Rolle der Datenmittler einhergehen, als auch um das Vertrauen in diese Organisationen zu erhöhen, sollten diese Dienste einem obligatorischen Zertifizierungssystem unterliegen.

Obligatorischer Genehmigungsrahmen für „datenaltruistische Organisationen“: Um ein höheres Maß an Vertrauen zu gewährleisten, sollte auch für datenaltruistische Organisationen ein obligatorischer Genehmigungsrahmen gelten. Außerdem sollte klargestellt werden, dass auch im

Rahmen des Datenaltruismus, bei Einwilligungen in die Verarbeitung von personenbezogenen Daten für Zwecke im allgemeinen Interesse, die keine Zwecke der wissenschaftlichen Forschung sind, stets ein festgelegter, eindeutiger und legitimer Zweck vorliegen muss.

Integrität, Aktualität und Verständlichkeit datenaltruistischer Organisationen muss konkret gewährleistet sein: Die allgemeinen Schutzanforderungen aus Art. 19 sind zu konkretisieren. Auch hier sollten die DSGVO-Anforderungen an Information und Einwilligung vollumfänglich zum Tragen kommen. Außerdem sollten Dateninhaber*innen nicht nur über eine etwaige Verarbeitung außerhalb der Union „informiert" werden, sondern auch über die damit einhergehenden Risiken. Diese betreffen die Nichteinhaltung von Datenschutzpflichten aufgrund unterschiedlicher rechtlicher Rahmenbedingungen und damit verbundener unzureichender Kontrollmöglichkeiten sowie eine möglicherweise unbeabsichtigte Stärkung bestehender Daten-Monopolisten. Des Weiteren sind Schutzmaßnahmen zu realisieren, dass nicht mit aggressiven, irreführenden Marketingpraktiken für Datenspenden geworben wird. Sanktionsmöglichkeiten sollten vorgesehen werden, wenn gegen Gemeinwohlinteressen gehandelt wird.

Zentrale Anforderungen an Datenintermediäre müssen verpflichtend gelten: Sie dürfen nicht allein in den Erwägungsgründen aufgeführt werden.

Persönlichkeitsrechte dürfen nicht zum Spielball wirtschaftlicher Interessen werden: Ein gesetzlicher Rahmen für die Nutzung von Daten muss die Kontrolle und den Schutz personenbezogener Daten sicherstellen. Die DSGVO sowie die nationalen Datenschutzgesetze müssen konsequent umgesetzt und auch bei neuartigen Angeboten angewendet werden. Damit die Rechte der betroffenen Personen gewahrt werden können, müssen die öffentliche Stellen, bevor die Daten weitergegeben werden, die Betroffenen in nachvollziehbarer Weise informieren (Grundsatz der Transparenz, Art. 5 Abs. 1 DSGVO). Auch weitere Anforderungen gemäß DSGVO, wie zum Beispiel Datenschutzfolgenabschätzung, Datensparsamkeit und Zweckbestimmung sind zu konkretisieren.

Nicht die Kapazitäten öffentlicher Einrichtungen überfordern: Öffentliche Stellen werden ohne konkreten Auftrag und entsprechende Ausstattung absehbar kaum in der Lage sein, die Ergebnisse der Datenverarbeitung zu prüfen und die Verwendung zu verbieten, wenn Informationen enthalten sind, die die Interessen und Rechte Dritter gefährden.

Rechtsdurchsetzung und Aufsicht wirksam gestalten: Innerhalb Europas aber auch insbesondere im außereuropäischen Bereich müssen die Rechtsdurchsetzung und Aufsicht verbessert, eine Zersplitterung der Rechtsauslegung vermieden werden sowie wirksame Sanktionen gegen Verstöße festgelegt werden. In Bezug auf Fragen, die eine Interpretation oder Prüfung der Einhaltung der DSGVO erfordern, sollten die für die Durchsetzung des DGA zuständigen Behörden stets zunächst eine Stellungnahme oder einen Beschluss der gemäß der DSGVO zuständigen Aufsichtsbehörden einholen und sich nach dieser Stellungnahme oder diesem Beschluss richten müssen.

Klärung von Haftungsfragen: Es bedarf der Definition klar abgegrenzter haftungsbegründender Verantwortlichkeiten der einzelnen Akteur*innen.

Klare Transparenz- und Datensicherheitspflichten schaffen: Dies gilt sowohl für „öffentliche" bzw. unterstützende „zuständige" Stellen sowie für die Datenintermediäre.

Bedeutsamkeit innovativer öffentlicher Infrastrukturen: Im Gesetzesentwurf unterbelichtet ist die Funktion des öffentlichen Dienstes, dem eine bedeutende Rolle bei der gemeinwohlorientierten Nutzung und Bereitstellung von Daten zukommen sollte. Dafür wäre der Aufbau von innovativen Infrastrukturen der öffentlichen Hand vonnöten, die diese erst in die Lage versetzen würde, selbst die Datensätze des öffentlichen Sektors für das Gemeinwohl zu verwerten und nutzbar zu machen.

Kostenwahrheit und Kostenklarheit schaffen: Statt Kosten, die der öffentlichen Hand durch eine möglichst sichere Zurverfügungstellung von Daten entstehen, klein zu rechnen und zudem betriebs- und volkswirtschaftliche Kosten-Nutzen-Kalkulationen zu vermischen, sollte eine realistische Berechnung von Personal- und Technikkosten vorgenommen werden. Wenn statt dezentral gespeicherten Daten und häufig noch mit Medienbrüchen versehenen Abläufen die Zugänglichkeit von Daten und die Schaffung von Datenpools gefördert wird, steigen die Sicherheitskosten, die auch fortlaufend auf den aktuellen Stand der Technik gebracht werden müssen, immens an.

Faire Wettbewerbschancen für kleine Unternehmen: Die Schaffung fairer Wettbewerbschancen für kleine Unternehmen – beispielsweise durch eine stärkere Regulierung großer „Datensammler" – zählt bisher nicht zu den Zielen des Entwurfes. Dies muss geändert werden. Die in engem Rahmen zulässigen Ausschließlichkeitsvereinbarungen dürfen aus diesem Grund keinesfalls mit den großen „Datensammlern" abgeschlossen werden.

Dateninnovationsrat stärken: Die Einrichtung eines europäischen Dateninnovationsrats ist als Ergänzung – und nicht zur Untergrabung – des europäischen Datenschutzausschusses begrüßenswert. Sinnvoll wäre zudem eine paritätische Besetzung, in der auch die Besonderheiten der digitalen Arbeitswelt durch gewerkschaftliche Beteiligung abgedeckt wären.

Anlage:

„Amendments by the United Services Union of Germany (ver.di) to the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)", eingereicht am 8. April 2021

8 April 2021

Amendments by the United Services Union of Germany (ver.di)

to the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

COM(2020) 767 final

With its proposal for a Regulation on **European Data Governance**, the European Commission intends to facilitate the processing of data while respecting fundamental European values.

ver.di welcomes in principle that *non-personal* data may be made available to strengthen the common good and the European Single Market, and to pave the way for innovative data trusts in the public interest.

However, ver.di takes a critical view of the transfer and external processing of explicitly sensitive public service data insofar as this could result in:

- weakening the trust of citizens in the collection and processing of data by the public administration,
- increasing the risk of data misuse,
- not sufficiently protecting employee data and the personal rights of citizens,
- boosting the concentration of data-based power, be it political or economic, and thus contribute to weakening the European internal market, and
- services of general interest coming under pressure to be privatised.

Furthermore, ver.di is critical of the fact that:

- the focus of data acquisition is not on private sector data, but on the (sensitive) data of the public sector, and that
- the proposal attaches only little importance to the use and processing of data for the common good.

From ver.di's point of view, it is therefore crucial to fundamentally revise the proposal in order to exclude the above-mentioned risks and to gear it to the common good and fundamental rights, to strengthen digital sovereignty from the local to the European level, and to counteract data monopolies.

In this sense, ver.di considers the following changes necessary.

Article 1 – Subject matter and scope

Commission's Proposal	Amendment by ver.di
Article 1 (2) This Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements related to processing of personal or non-personal data. Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply.	**Article 1** (2) This Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements related to processing of personal or non-personal data. Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply. ***Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) applies to any form of further use of data. In this respect, sensitive personal data shall not be re-used for security reasons.*** ***(2a) (new) The re-use of employee data shall be prohibited. To this end, it must be ensured that public service data do not contain employee data, such as in the area of mobility.***
Explanation According to Recital 6 of the Commission's proposal, "the processing of personal data should rely upon one or more of the grounds for processing provided in Article 6 of Regulation (EU) 2016/679". The term 're-use', however, is defined in Article 2 (2) as use of data "for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced". Therefore, it should be clearly stated in Article 1 (2) that the re-use of personal data is prohibited.	

Article 3 – Categories of data

Commission's Proposal	Amendment by ver.di
Article 3 (1) This Chapter applies to data held by public sector bodies which are protected on grounds of: (a) commercial confidentiality; (b) statistical confidentiality; (c) protection of intellectual property rights of third parties; (d) protection of personal data.	**Article 3** (1) This Chapter applies to data held by public sector bodies which are protected on grounds of: (a) commercial confidentiality; (b) statistical confidentiality; (c) protection of intellectual property rights of third parties; ~~***(d) protection of personal data.***~~

Commission's Proposal	Amendment by ver.di
Explanation On the one hand, the GDPR already covers the area of personal data. On the other hand, according to Recital 6 of the Commission's proposal, personal data should be made available for further use through "techniques enabling privacy-friendly analyses on databases that contain personal data". As long as de-personalisation techniques are not sufficiently developed and the risks of re-personalisation are too high, personal data should be excluded from the scope of this Regulation. Research into effective anonymisation tools should be intensified. In the long term, any disclosure of personal data that causes a change of purpose of already processed data should be subject to an anonymisation obligation.	

Commission's Proposal	Amendment by ver.di
Article 3 (2) This Chapter does not apply to: (a) data held by public undertakings; (b) data held by public service broadcasters and their subsidiaries […]; (c) data held by cultural establishments and educational establishments; (d) data protected for reasons of national security , defence or public security; (e) data the supply of which […].	**Article 3** (2) This Chapter does not apply to: (a) data held by public undertakings; (b) data held by public service broadcasters and their subsidiaries […]; (c) data held by cultural establishments and educational establishments; (d) data protected for reasons of national security , defence or public security; (e) data the supply of which […]. ***(f) data processed in the context of employment.***
Explanation Personal employee data and, if applicable, other data from the context of employment must be excluded from the scope of this chapter in order to ensure that they do not fall below the protection according to Article 6, 88 and others of the GDPR. There are far-reaching possibilities for further processing of employee data already today. For example, according to Article 7 of the GDPR, data processing can regularly take place on the basis of voluntary consent. In this respect, there is no need for further regulation.	

Article 5 – Conditions for re-use

Commission's Proposal	Amendment by ver.di
Article 5 (2) Conditions for re-use shall be non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed. These conditions shall not be used to restrict competition.	**Article 5** (2) Conditions for re-use shall be non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed. ***~~These conditions shall not be used to restrict competition.~~***
Explanation	

Commission's Proposal	Amendment by ver.di
Competitiveness lacks a clear definition. The term is vague and does not provide legal certainty. Therefore, it is not suitable as a basic condition and should be deleted.	

Commission's Proposal	Amendment by ver.di
Article 5 (3) Public sector bodies may impose an obligation to re-use only pre-processed data where such pre-processing aims to anonymize or pseudonymise personal data or delete commercially confidential information, including trade secrets.	**Article 5** (3) Public sector bodies ***shall*** impose an obligation to re-use only pre-processed ***non-personal*** data ~~***where such pre-processing aims to anonymize or pseudonymise personal data or delete commercially confidential information, including trade secrets***~~ ***and that data containing trade secrets are processed accordingly. It must be ensured that companies do not have direct access to protected data and that, as a consequence, anonymization or pseudonymisation cannot be carried out by them.***
Explanation Effective and secure anonymisation procedures are a prerequisite for further use of personal data. Apart from this, the Commission's proposal leaves it open who carries out the anonymisation or pseudonymisation. Therefore, it must be ruled out that companies could get direct access to protected data. Remote access to protected data may only be realised with the prior consent of the data subjects.	

Commission's Proposal	Amendment by ver.di
Article 5 (4) Public sector bodies may impose obligations (a) to access and re-use the data within a secure processing environment provided and controlled by the public sector; (b) to access and re-use the data within the physical premises in which the secure processing environment is located, if remote access cannot be allowed without jeopardising the rights and interests of third parties.	**Article 5** (4) Public sector bodies ***shall*** impose obligations (a) to access and re-use the data within a secure processing environment provided and controlled by the public sector; (b) to access and re-use the data within the physical premises in which the secure processing environment is located~~***, if remote access cannot be allowed without jeopardising the rights and interests of third parties***~~ ***in accordance with high security standards to be established and continuously monitored.***
Explanation High security standards are the prerequisite for the access and re-use of the data within physical premises.	

Commission's Proposal	Amendment by ver.di
Article 5 (5) The public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body shall be able to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties.	**Article 5** (5) The public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body shall be able to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. ***To this end, the public sector bodies shall be equipped with the necessary human and financial resources for monitoring and law enforcement.***
Explanation The Member States must ensure adequate funding for their public sector bodies.	

Commission's Proposal	Amendment by ver.di
Article 5 (9) The Commission […]. (10) Public sector bodies […]. (11) Where specific Union acts […]. (12) The natural or legal person […]. (13) Where the re-user […].	**Article 5** ~~***(9) The Commission […].***~~ ~~***(10) Public sector bodies […].***~~ ~~***(11) Where specific Union acts […].***~~ ~~***(12) The natural or legal person […].***~~ ~~***(13) Where the re-user […].***~~
Explanation An authorisation of the Commission to adopt implementing acts for the further use of data to third countries must be ruled out. This is also contradictory to Recital 3 of the Commission's proposal that states the necessity "to improve the conditions for data sharing in the internal market". In terms of anonymisation and pseudonymisation of personal data, the Commission's proposal notes in Article 5 (11) that there may be "risks of re-identification of anonymized data for data subjects". As long as there are security risks, the re-use of these data should be ruled out.	

Article 6 – Fees

Commission's Proposal	Amendment by ver.di
Article 6 (2) Any fees shall be non-discriminatory, proportionate and objectively justified and shall not restrict competition.	**Article 6** (2) Any fees shall be non-discriminatory, proportionate and objectively justified and shall ~~***not restrict competition***~~ ***cover the costs of monitoring and enforcement. They shall not create incentives to sell or lower the protection of sensitive data.***

Article 7 – Competent bodies

Commission's Proposal	Amendment by ver.di
Article 7 (4) The competent body or bodies shall have adequate legal and technical capacities and expertise to be able to comply with relevant Union or national law concerning the access regimes for the categories of data referred to in Article 3 (1).	**Article 7** (4) The competent body or bodies shall have adequate ***human resources as well as*** legal and technical capacities and expertise to be able to comply with relevant Union or national law concerning the access regimes for the categories of data referred to in Article 3 (1)***, so that data protection, privacy and confidentiality are fully respected. The competences and resources of the competent body or bodies shall prohibit unjustifiable outsourcing.***

Article 9 – Providers of data sharing services

Commission's Proposal	Amendment by ver.di
Article 9	**Article 9** ***(2a) (new) A mandatory certification system shall be provided for data intermediaries in order to limit the risks associated with the central role of data intermediaries and thus increase trust in these organisations and their activities.***

Article 19 – Specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data

Commission's Proposal	Amendment by ver.di
Article 19 (1) Any entity entered in the register of recognised data altruism organisations shall inform data holders: (a) about the purposes of general interest for which it permits the processing of their data by a data user in an easy-to-understand manner; (b) about any processing outside the Union.	**Article 19** ***(-1a) (new) A mandatory authorisation framework for data altruistic organisations shall be provided to ensure a higher level of trust.*** (1) Any entity entered in the register of recognised data altruism organisations shall inform data holders: (a) about the purposes of general interest for which it permits the processing of their data by a data user in an easy-to-understand manner; (b) about any processing outside the Union ***and associated risks***.
Explanation	

Commission's Proposal	Amendment by ver.di
Such risks with regards to any processing outside the Union concern non-compliance with data protection obligations due to different legal conditions and a related lack of sufficient control possibilities as well as a possibly unintended boost of existing monopolies.	

Commission's Proposal	Amendment by ver.di
Article 19 (2) The entity shall also ensure that the data is not be used for other purposes than those of general interest for which it permits the processing.	**Article 19** (2) The entity shall also ensure that the data is not be used for other purposes than those of general interest for which it permits the processing. ***Safeguards shall be provided to ensure that misleading marketing practices are not used to solicit donations of data. Possibilities for sanctions shall be provided for when acting against public interests.***