AK EUROPA

Positionspapier
Dezember 2023
Konsument:innen

Financial Data Access

COM(2023) 360

Zusammenfassung

Zum Hintergrund

Der Vorschlag zielt – vergleichbar mit den bereits veröffentlichten Vorschlägen der Kommission zum EU-Gesundheitsdatenraum und zum Datengesetz – auf den Zugang zu personenbezogenen Finanzdaten sowie deren Austausch und Nutzung durch verschiedene Datennutzer ab. Erklärtes Ziel ist es, einen „Mehrwert" in Form von Innovationen im EU-weiten Finanzdienstleistungssektor zu generieren.

Zusammenfassende Bewertung

- Es braucht eine bessere Balance zwischen den Interessen der Datenökonomie und jenen der Konsument:innen. Die AK fordert u.a. einen eigenen Legislativakt, der Unternehmen im Allgemeinen und Wirtschaftsauskunfteien im Speziellen präzise Grenzen für die Nutzung von Finanz- und Verhaltensdaten zu Zwecken der Bonitätsbewertung und -prognose setzt.

- Es ist klarzustellen, dass Versicherungsprodukte mit Gesundheitsbezug und Daten über die Kreditwürdigkeit von Konsument:innen nicht vom Anwendungsbereich des Entwurfs erfasst sind. Art 2 hält dies zwar unmissverständlich fest; Art 7 schafft für die ausgenommenen Bereiche dennoch Leitlinienkompetenzen der EU-Kommission.

- Die bruchstückhafte Wiedergabe von Auszügen aus der DSGVO sollte vermieden werden. Es entsteht dadurch kein Mehrwert, dafür aber unnötige Rechtsunsicherheit bezüglich der Zuständigkeiten der Datenschutz- oder Finanzaufsichtsbehörden.

- Wünschenswert wären über die allgemeinen Grundsätze der DSGVO hinausgehende präzise sektorspezifische Vorgaben, etwa zu Informations- und Zustimmungsrechten, zur Zweckbindung, zur Datensicherheit und zu Werbeverboten.

- Der undefinierte Begriff „Berechtigung" zieht sich durch den gesamten Entwurf. Er sollte durch den eindeutig definierten Begriff „Zustimmung" unter Verweis auf die DSGVO ersetzt werden.

- „Systeme zur gemeinsamen Nutzung von Finanzdaten" sollten angehalten sein, personenbezogene Daten auf Servern und in Clouds zu speichern, die sich innerhalb der EU befinden.

- Bei der Festlegung der zuständigen Behörden wäre explizit darauf hinzuweisen, dass die Datenschutzbehörden sämtliche aus der Verordnung resultierende Aspekte des Datenschutzes zu vollziehen haben.

- Die Herausgabe von Verkehrsdaten der Telekommunikationsbetreiber sollte mangels Konformität mit der EUGH-Rechtsprechung ersatzlos gestrichen werden.

Die Position der AK

Allgemeines

Die Ambitionen des Vorschlags stehen zwangsläufig in einem Spannungsverhältnis zu den Grundrechten auf Datenschutz und Privatsphäre, die grundsätzlich Vorrang vor rein wirtschaftlichen Interessen haben.. Die Förderung von Wettbewerb und neuen Finanzdienstleistungsprodukten ist dabei durchaus als berechtigtes Interesse anzuerkennen. Beides stellt jedoch i.d.R. kein überwiegendes berechtigtes Interesse im Sinne der DSGVO dar, hinter dem die Geheimhaltungsinteressen der Konsument:innen pauschal und undifferenziert zurücktreten müssten. Konsument:innen müssen frei darüber entscheiden können, ob es etwa auf ihr persönliches Profil zugeschnittene Angebote geben soll, für die sie ihre Finanz- und Verhaltensdaten Dritten überlassen. Die digitale Selbstbestimmung der Konsument:innen ist die oberste Maxime: Ob, welche und zu welchem konkreten Zweck Finanzdaten untereinander geteilt werden dürfen, sind Entscheidungen, die ausschließlich den Konsument:innen vorbehalten sind. Auch wenn der Entwurf – soweit erkennbar – durchgängig auf dem Zustimmungserfordernis der Konsument:innen zur Datennutzung aufbaut, ist zu klären, ob Konsument:innen die Tragweite ihrer Entscheidung und die einzelnen Datenflüsse in einer technisch hochkomplexen Marktsituation hinreichend überblicken können.

Der Entwurf ist deshalb auch daran zu messen, ob er die elementaren Prinzipien der DSGVO beachtet: Etwa den Grundsatz der Datensparsamkeit sowie aussagekräftige Vorabinformationen über Datennutzungen, auf deren Grundlage die Konsument:innen informiert und frei – also ohne Nachteil – entscheiden können, ob sie zustimmen oder nicht. Die Opinion 38/2023 des EU-Data Protection Supervisor (EDPS) vom 22.8.2023 macht richtigerweise auf das erhebliche Kräfteungleichgewicht zwischen Konsument:innen und Finanzinstituten aufmerksam. Wer rasch einen Kredit benötigt oder auf eine bestimmte Versicherung im Alltag angewiesen ist, ist jedenfalls die deutlich schwächere Vertragspartei. An der Freiwilligkeit und damit der Wirksamkeit der abgegebenen Willenserklärung bestehen deshalb regelmäßig Zweifel. Es ist ein augenscheinliches Defizit des Entwurfes, dass er keine die DSGVO konkretisierenden Kriterien enthält, anhand derer festgestellt werden kann, ob eine Zustimmung zu einem datengetriebenen Vorhaben überhaupt gültig sein kann. Mehr noch: Der EDPS kritisiert in seiner Stellungnahme (S. 10, „The role of permissions"), dass mit der Umschreibung „permissions of the customer" unnötigerweise ein neuer Begriff eingeführt wird, der sich offensichtlich von der datenschutzrechtlichen Zustimmung (DSGVO; „consent") unterscheidet. Die damit verfolgte Absicht ist unklar und bedarf jedenfalls der Klärung.

Grundsätzliche Kritik

Die AK beurteilt den Vorschlag aus mehreren Gründen sehr kritisch:

- Der von der Kommission proklamierte Handlungsbedarf, weil Kund:innen im Zugang zu ihren Daten behindert sind, ist nicht nachvollziehbar. In der Konsumenten:innen-Beratung der AK wurden bisher keine Beschwerden über mangelnden Datenzugang registriert. Es handelt sich bei diesen Daten zumeist um Vertragsdaten und vertragliche Informationen, zu denen Kund:innen jedenfalls Zugang haben, sei es online oder in Papierform.

- Finanzdienstleistungen sind sehr komplexe Produkte und ein äußerst sensibler Bereich. Einerseits, weil es sich regelmäßig um Verträge mit sehr hohen Geldbeträgen handelt, die Verbraucher:innen nur einmal in ihrem Leben abschließen (Hypothekarkredite oder Pensionsvorsorge) oder die mit einem Verlustrisiko behaftet sind, wie viele Geldanlageprodukte. Andererseits geht es um lebenslange Verträge wie private Krankenversicherungen bzw. um Verträge, die der Absicherung von existentiellen Risiken dienen (Eigenheim-, Haftpflicht- und Unfallversicherungen).

- Im Vertrieb von Finanzdienstleistungen spielen Provisionen europaweit aktuell noch immer

eine erhebliche Rolle. Negative Anreize und deren Auswirkungen wurden u.a. von der BEUC dokumentiert. Die Legislativvorschläge zur Kleinanlegerstrategie ändern nichts Wesentliches an diesen Vertriebsstrukturen. Es ist zu befürchten, dass der vorgeschlagene weitreichende Zugang zu Finanzdaten das Risiko aggressiver Vertriebspraktiken, wie bspw. das selbst von der Versicherungsbranche oft beklagte „Ausspannen" von Versicherungsanlageprodukten, signifikant erhöhen wird.

- Im digitalen Zeitalter ist grundsätzlich von permanenter Verletzlichkeit auszugehen. Die Annahme, dass Verbraucher:innen souverän handeln, wenn ihnen detaillierte Informationen zugänglich sind, ist überholt. Das Vertrauen jedes/r Einzelnen kann in der Digitalökonomie leicht ausgenutzt werden. Manipulation, Missbrauch und „Social Engineering" etwa im Bereich des Online-Zahlungsverkehrs haben in den letzten Jahren zu einem starken Anstieg von Schäden geführt, die letztlich die Kund:innen zu tragen hatten. Der Entwurf der Kommission ist geprägt vom Leitbild der informierten, verständigen und sorgfältigen Verbraucher:innen, obwohl eine Abkehr von diesem Leitbild insbesondere auch in der Gesetzgebung notwendig ist. Stattdessen ist in Zukunft von permanent verletzlichen Verbraucher:innen auszugehen.

Zu den wesentlichen Bestimmungen des Entwurfs: Der Anwendungsbereich

Die Liste umfasst eine enorme Bandbreite an Kundendaten wie Hypothekarkreditverträge, Darlehen und Konten (mit Ausnahme von Zahlungskonten im Sinne der Zahlungsdiensterichtlinie), einschließlich (Spar-)Guthaben, Konditionen und Transaktionen, (versicherungsbasierte) Anlageprodukte, Krypto-Vermögenswerte und Immobilien. Außerdem die Bonitätsbeurteilung von Unternehmen im Falle eines Kreditantrags.

Bonitätsauskünfte: Dass Bonitätsbeurteilungen von Konsument:innen nicht erfasst sind, wird ausdrücklich begrüßt. Zugleich macht die AK aber darauf aufmerksam, dass dringender Bedarf an einer EU-weit einheitlichen datenschutzrechtlichen Regulierung des Gewerbes von Wirtschaftsauskunfteien und den von ihnen (mit oder ohne KI-Systemen) erstellten Bonitätsbewertungen besteht. Begründend wird angemerkt, dass die DSGVO deren Geschäftspraktiken (in Bezug auf Datenquellen, Datenumfang, Vorabinformation der Betroffenen, Einsatz von und Auskünfte über automatisierte Einzelentscheidungen, Prüfung der Abfrageberechtigung von Datenempfängern, Speicherdauer und Umgang mit Berichtigungsansprüchen) nicht annähernd vereinheitlicht hat. Rechtswidrige Datennutzungen (z.B. Datenbezug von Direktwerbeunternehmen oder aus sozialen Medien), mangelhafte Datenqualität, unwissenschaftliche und damit diskriminierungsgeneigte Scoringmethoden verletzen viele Konsument:innen in ihren Grundrechten und schließen sie oft völlig ungerechtfertigt durch schlechte Bewertungen von der Teilhabe am Geschäftsleben aus.

Versicherungsprodukte mit Gesundheitsbezug: Wir schließen uns der Haltung des EDPS an: Es ist zu begrüßen, dass Lebens- und Krankenversicherungen aufgrund der hohen Sensibilität der dabei anfallenden Daten vom Anwendungsbereich ausgenommen sind.

AK-Anliegen: Der vorliegende Entwurf ist zwar nicht unmittelbar geeignet, verbraucherfreundliche gesetzliche Anforderungen an Bonitätsbewertungen aufzunehmen. Die AK hält aber eine eigene sektorspezifische Richtlinie zur Regulierung von Bonitätsbewertungen und KI-basierten Scorings des Verhaltens von Konsument:innen für überfällig. Nicht zuletzt, weil mit dem geplanten Finanzdatenraum viel mehr Verhaltensdaten zur Verfügung stehen, die für Bonitätsanalysen besonders attraktiv wären. Der Verwertbarkeit der vom Entwurf erfassten Daten für Bonitätsbewertungen und -prognosen sind daher angemessene Grenzen zu setzen. Nur so wäre ein fairer Ausgleich zwischen der Förderung der Datenökonomie durch den Zugang zu personenbezogenen Finanzdaten und den Schutzbedürfnissen der Konsument:innen vor benachteiligenden Bewertungen geschaffen.

Verpflichtung der Dateninhaber, den Datennutzern Kundendaten zur Verfügung zu stellen

Auf Kundenwunsch hat der Dateninhaber Datennutzern Daten für jene Zwecke zu überlassen, für die der Kunde seine Erlaubnis erteilt hat. Davor hat der Dateninhaber den Datennutzer aufzufordern, nachzuweisen, dass er die Erlaubnis des Kunden zum Zugriff auf die beim Dateninhaber gespeicherten Kundendaten erhalten hat. Außerdem ist dem Kunden ein Dashboard zur Überwachung und Verwaltung der Berechtigungen zur Verfügung zu stellen.
Der Begriff „Erlaubnis" (permission) wird nicht näher definiert und unterscheidet sich auch vom Bedeutungsgehalt von der „Zustimmung" (consent), die eine Rechtsgrundlage für die Datenverarbeitung nach der DSGVO darstellt.

AK-Anliegen: Diese begrifflichen Abweichungen führen zu unnötiger Rechtsunsicherheit und entfalten im Übrigen auch keinerlei Nutzen. Dateninhaber und -nutzer sind und bleiben Verantwortliche im Sinne der DSGVO und haften jedenfalls für rechtswidrige Datenübermittlungen und -verarbeitungen, die nicht von einer gültigen Zustimmung der Konsument:innen gedeckt sind. Auch andere datenschutzrechtliche Rechtsgrundlagen als die Zustimmung dürften nicht in Betracht kommen, da der Entwurf Konsument:innen ausnahmslos ein Widerrufsrecht zugesteht, das die DSGVO nur in Verbindung mit der Rechtsgrundlage einer „Zustimmung" vorsieht. Aus Sicht der AK sollte deshalb der Datennutzer vom/von der Konsument:in eine datenschutzrechtlich wirksame Zustimmung einholen müssen. Der Dateninhaber sollte vor der Weitergabe der Daten die unterfertigte Einwilligungserklärung anfordern und ihre Wirksamkeit und Reichweite prüfen müssen. Ist sie unpräzise formuliert, hat er den Datennutzer zur Nachbesserung aufzufordern. Außerdem sollte der Dateninhaber prüfen müssen, ob der Datennutzer eine Ausübungsberechtigung iSd Art 6 Abs 1 besitzt.

Pflichten eines Datennutzers, der Kundendaten erhält

Nach Art 6 Abs 2 darf der Datennutzer auf Kundendaten nur für die Zwecke und unter den Bedingungen zugreifen, für die der Kunde seine Zustimmung erteilt hat. Er muss sie löschen, wenn sie nicht mehr erforderlich sind. Der Mehrwert dieser Anordnung, die sich ohnehin unmittelbar aus der DSGVO ergibt, erschließt sich nicht. Sollte die redundante Aufnahme datenschutzrechtlicher Pflichten des Auftraggebers nach der DSGVO im vorliegenden Entwurf dazu dienen, neben den Datenschutzbehörden auch die Aufsichtsbehörden für den Finanzsektor als datenschutzrechtliche Prüforgane vorzusehen, dann wäre es zweckmäßiger, dies bei den Aufsichtszuständigkeiten zu thematisieren (und die genauen Aufgabengebiete und Pflichten zur Zusammenarbeit der Behörden präzise zu bestimmen).

In Art 6 Abs 4 wird der Datennutzer (redundant) nochmals verpflichtet, „keine Kundendaten zu anderen Zwecken als zur Erbringung der vom Kunden ausdrücklich angeforderten Dienstleistung [zu] verarbeiten", und zwar mit der Begründung, „eine wirksame Verwaltung der Kundendaten zu gewährleisten." Diese Begründung ist nicht nachvollziehbar, „to ensure the effective management of data" ist eine Leerformel. Es wird verabsäumt, die Verantwortung des Datennutzers hervorzuheben, (selbstverständlich) die Grundrechte (der Kund:innen eines Dritten) achten zu müssen.

Ebenso vermissen wir legistische Qualität bei der Formulierung der Punkte c) und d). Demnach sind „angemessene technische, rechtliche und organisatorische Maßnahmen zu ergreifen, um die [...] unzulässige Übermittlung von oder den Zugang zu nicht personenbezogenen Kundendaten zu verhindern" sowie „die erforderlichen Maßnahmen zu ergreifen, um ein angemessenes Sicherheitsniveau bei der Speicherung, Verarbeitung und Übermittlung nicht personenbezogener Kundendaten zu gewährleisten". Warum in beiden Fällen der Schutz nicht-personenbezogener Daten im Mittelpunkt steht, obwohl der Entwurf aufgrund der Art der Daten (Kundendaten) und der Rechtsgrundlage (Zustimmungserfordernis nach der DSGVO) durchwegs personenbezogene Daten anspricht, erschließt sich nicht. Unklar bleibt zudem, warum nicht auch Datensicherheitsmaßnahmen für personenbezogene Daten verlangt werden.

Viel mehr als – man möchte fast sagen – Pseudo-Schutz ist auch von der Anforderung an die Datennutzer in Punkt e) nicht zu erwarten. Demnach dürfen Kundendaten nicht zu Werbezwecken verarbeitet werden, „es sei denn, sie dienen dem Direktmarketing im Einklang mit dem Unionsrecht und dem nationalen Recht". Dass Direktmarketing nur im Rahmen der nationalen und europäischen Gesetze zulässig ist, bedarf keiner weiteren Erwähnung. Welche anderen denkbaren Werbeformen über das Direktmarketing hinaus ausgeschlossen werden sollen, bleibt im Dunkeln. Schließlich sei noch angemerkt, dass es keine durch EU-Rechtsakte vereinheitlichte Definition von Direktmarketing gibt (nur Werbung für eigene Produkte des Datennutzers oder auch jene Dritter; im Falle von Dritten stellt sich die vom EuGH noch nicht geklärte Rechtsfrage zu EG 47 der DSGVO: Demnach kann Direktwerbung ein berechtigtes Interesse darstellen, wobei unklar ist, ob dies nur eigene Kunden des Datenverantwortlichen betrifft, die mit seinen eigenen Produkten beworben werden, oder auch Direktwerbung durch Dritte, die mit dem/der Konsument:in in keiner Vertragsbeziehung stehen).

AK-Anliegen: Die Wiedergabe von kurzen, unvollständigen Auszügen aus der DSGVO im vorliegenden Entwurf bringt den betroffenen Konsument:innen keinerlei Mehrwert. Sie führt jedoch zu erheblichen und unerwünschten Rechtsunsicherheiten, welche Behörde (Datenschutz- oder Finanzaufsichtsbehörden) für den Vollzug dieser Pflichten zuständig ist. Im Interesse des Konsument:innenschutzes erwartet sich die AK präzisere, über die allgemeinen DSGVO-Grundsätze hinausgehende sektorspezifische Vorgaben zur Einholung der Zustimmung, zur Begrenzung der

Verwendungszwecke, zur Datensicherheit und zum Werbeverbot.

Umfang der Datennutzung

Der Entwurf erinnert daran, dass die Verarbeitung von Kundendaten auf das für die Zwecke, für die sie verarbeitet werden, erforderliche Maß zu beschränken ist. Dieser Hinweis deckt sich mit dem Grundsatz der Datensparsamkeit nach der DSGVO, ohne über ihn hinauszugehen und ihn zu präzisieren. Wie schon bei Art 6 kritisiert, wird hier eine Norm ohne Mehrwert geschaffen, die aber zu Rechtsunsicherheiten führt. Positive wie negative Kompetenzkonflikte sind zu erwarten (zwei oder keine sich zuständig erachtende Behörde; Datenschutz- vs. Finanzaufsichtsbehörden).

Vor diesem Hintergrund lehnt die AK auch entschieden die Ermächtigung der Europäischen Bankenaufsichtsbehörde (EBA) ab, „Leitlinien für die Umsetzung von Absatz 1 dieses Artikels für Produkte und Dienstleistungen, die mit der Kreditwürdigkeit des Verbrauchers in Zusammenhang stehen" zu entwickeln bzw. der Versicherungsaufsichtsbehörde (EIOPA) in Fällen, „die mit der Risikobewertung und Preisfestsetzung für einen Verbraucher im Falle von Lebens-, Kranken- und Gesundheitsversicherungsprodukten verbunden sind". Erstens eignen sich Aufsichtsbehörden für einzelne Wirtschaftssektoren Kompetenzen an, die im Aufgabenbereich der unabhängigen Datenschutzbehörden liegen. Die vorgesehene Zuziehung des Datenschutzausschusses schafft keinen angemessenen Ausgleich für diese Kompetenzverschiebung. Beide Behörden sind ausschließlich auf den Bedarf der Wirtschaftsteilnehmer fokussiert, nicht aber auf die Datenschutz- und Privatsphärenrechte der Konsument:innen. Es ist daher nur denkbar, dass der Datenschutzausschuss federführend ist und im Zusammenwirken mit der EBA bzw. EIOPA Leitlinien dazu erlässt.

Zweitens stellt sich die Frage, warum generell auf Abs 1 verwiesen wird, der sich wiederum auf Art 2 Abs 1 bezieht, wenn die Leitlinien den angemessenen Datenumfang nur für äußerst spezifische Bereiche (die Kreditwürdigkeit der Verbraucher und die Risikobewertung bei Lebens- und Krankenversicherungen) festlegen sollen, die von Art 2 Abs 1 gar nicht erfasst sind. Mit anderen Worten stellt sich die ganz entscheidende Frage, warum überhaupt Leitlinien ermöglicht werden zu Datenkategorien, die nicht in den Anwendungsbereich der Verordnung fallen: Nach Art 2 Abs 1 f) sind nämlich nur Kreditwürdigkeitsprüfungen von Unternehmen erfasst, nicht aber solche von Verbraucher:innen. Nach Art 2 Abs 1 e) sind Versicherungen grundsätzlich erfasst – mit Ausnahme der Lebens-, Kranken- und vergleichbaren gesundheitsbezogenen Versicherungen.

AK-Anliegen: Noch deutlicher als in Art 6 überschneiden sich Aufgaben der Datenschutzbehörden mit jenen der Finanzaufsicht, wenn bruchstückhaft und ohne jeglichen Mehrwert für Konsument:innen Grundsätze aus der DSGVO wiedergegeben werden. Die EBA soll explizit Leitlinienkompetenz für eine Aufgabe erhalten, die in den Kernbereich der DSGVO und damit des vollziehenden EU-Datenschutzausschusses fällt (Datensparsamkeit, Grenzen der für verschiedene Zwecke erforderlichen Daten). Eine derartige Kompetenzüberschreitung wird seitens der AK entschieden abgelehnt. Denkbar wäre, den EU-Datenschutzausschuss mit Leitlinienkompetenzen zu betrauen, wobei EBA bzw. EIOPA bei der Wahrnehmung dieser Aufgabe beizuziehen wären. Im konkreten Fall sollten sich die Leitlinien (selbstverständlich) auch nur auf Datenkategorien erstrecken, die überhaupt in den Anwendungsbereich des Entwurfes fallen. Bonitätsscores von Konsument:innen, Risikobewertung und Prämienfestlegung bei Lebens- und Krankenversicherungen zählen jedenfalls nicht dazu, weshalb diese Normteile ersatzlos entfallen müssten.

Dashboards mit Zugriffsrechten auf Finanzdaten

Der Dateninhaber soll Kund:innen ein Dashboard zur Verfügung stellen, um die den Datennutzern erteilten Berechtigungen zu überwachen und zu verwalten. Wir verweisen nochmals darauf, dass der Begriff „Berechtigung" nicht zwangsläufig dieselbe Bedeutung hat wie eine datenschutzrechtliche Zustimmung (permission – consent). Es ist klarzustellen, worin die Unterschiede bestehen, andernfalls sind Konsument:innenrechte in der Praxis nicht rechtssicher ausübbar. Die Geltungsdauer der Zugriffsberechtigung muss am Dashboard angegeben werden (Art 8 Abs 2 lit a v). Der Zeitraum der Zugriffsberechtigung ist allerdings nicht unbedingt derselbe wie für die erlaubte Speicherdauer der Daten. Hierfür sind ebenfalls Privacy-by-Design-Einstellungen nötig, um den Konsument:innen eine selbstbestimmte Wahl zu ermöglichen.

AK-Anliegen: Da es – soweit ersichtlich – im Entwurf ausschließlich um das Teilen personenbezogener Daten geht, sollte konsequenterweise der Terminus „Berechtigung" durch „Zustimmung" unter Verweis auf die DSGVO ersetzt werden. Auch Dateninhaber und -nutzer sollten eigentlich als Datenverantwortliche

und -empfänger im Sinn der DSGVO behandelt und bezeichnet werden, da sie ja jedenfalls Adressaten der DSGVO sind und ihren diesbezüglichen Pflichten nachkommen müssen (sollte es am Rande auch um aggregierte, „sonstige" Daten ohne Personenbezug gehen, würde es ausreichen, nur an diesen Stellen von Dateninhaber und -nutzer zu sprechen). Unabhängig von der jederzeit bestehenden Möglichkeit der Ausübung des Widerrufsrechtes durch die Konsument:innen sollte die maximale Speicherdauer für jede Datenkategorie am Dashboard ausgewiesen werden. Konsument:innen sollten die Möglichkeit erhalten zu entscheiden, ob sie nach der Zweckerfüllung eine physische Datenlöschung wünschen oder einer Weiterverarbeitung für Sekundärnutzungen über den ursprünglichen Zweck hinaus (etwa für statistische Zwecke) zustimmen.

Systeme zur gemeinsamen Nutzung von Finanzdaten

Die IT-Infrastruktur zum Austausch von Finanzdaten gehört zu den sensiblen Bereichen der Daseinsvorsorge, die in den Geltungsbereich der EU-NIS-Richtlinie fallen. Diese soll eine nationale und EU-weite Resilienz gegenüber Hackerangriffen und Störungen der Versorgungssicherheit gewährleisten, damit die Konsument:innen bzw. die Gesellschaft als Ganzes nicht durch Netzausfälle oder Datenmissbrauch betroffen und geschädigt werden. Die geplanten Systeme dürften wohl ein äußerst attraktives Ziel für Angreifer darstellen und sind daher in besonderem Maß unter dem Aspekt der Datensicherheit zu bewerten. Vor diesem Hintergrund ist es verwunderlich, dass die Netz- und Datensicherheit völlig ausgeklammert werden. Gemeinsame technische Standards betreffen nur die Interoperabilität. Systeme für den Austausch von Finanzdaten haben zwar die vertragliche Haftung der Mitglieder festzulegen, wenn die Datensicherheit beeinträchtigt ist oder die Daten missbraucht werden (bei personenbezogenen Daten richten sich die Haftungsbestimmungen nach der DSGVO). Aus Sicht der AK ist es ein Defizit des Entwurfes, dass überhaupt keine Maßnahmen zur Prävention von Missbrauch vorgesehen sind. Außerdem ist nicht nachvollziehbar, ob beim Aufbau solcher Austauschsysteme auf eine DSGVO-konforme Datenverarbeitung in Drittstaaten geachtet wird. Bislang überantworten Banken den internationalen Austausch elektronischer Informationen der "Society for Worldwide Interbank Financial Telecommunication" (SWIFT). Deren Nutzung von US-Servern als Speicherplatz für massenhaft sensible Zahlungstransaktionsdaten bei Auslandsüberweisungen wurde vielfach kritisiert.

AK-Anliegen: Im Lichte der EuGH-Entscheidungen zur Rechtswidrigkeit des auf diversen Übereinkommen wie dem Privacy Shield bzw. Standardvertragsklauseln basierenden Datentransfer zwischen der EU und den USA böte sich die Gelegenheit, die Datenspeicherung innerhalb der EU zu forcieren. Eine Verpflichtung zur Speicherung auf Servern und in Clouds innerhalb der EU wäre wünschenswert.

Zuständige Behörden

Die Wahl der zuständigen Behörden sollte den Mitgliedstaaten nur insoweit freistehen, als es sich nicht um die Vollziehung datenschutzrechtlicher Aufgaben handelt. Letztere sind den Datenschutzbehörden vorbehalten, worauf im Entwurf ausdrücklich hingewiesen werden sollte. Zu den Vollzugsaufgaben zählt u.a. auch, soweit dies nach nationalem Recht zulässig ist, „Verkehrsdaten von Telekommunikationsbetreibern anzufordern, wenn ein begründeter Verdacht auf einen Verstoß besteht und diese Aufzeichnungen für die Untersuchung eines Verstoßes gegen diese Verordnung von Bedeutung sein können".

Verkehrsdaten unterliegen dem Kommunikations-geheimnis der e-Privacy-Richtlinie. Als solche sind sie nur unter strengen rechtsstaatlichen Kautelen für andere als Abrechnungszwecke auswertbar. Der EUGH hat einer „Vorratsdatenspeicherung" von Verkehrsdaten für Zwecke der Strafverfolgung bereits mehrfach eine Absage erteilt. Vor diesem Hintergrund sind diese Daten nach dem Zustandekommen der Verbindung bzw. spätestens nach der Rechnungslegung zu löschen. Für eine nationale Zugriffserlaubnis besteht daher in der Praxis kaum ein relevanter Spielraum. Die Ermächtigungsnorm im vorliegenden Entwurf entspricht außerdem nicht der EuGH-Judikatur, die präzise Vorgaben für Grundrechtseingriffe verlangt. Vage Formulierungen wie „begründeter Verdacht" oder „[kann] für Untersuchungen von Bedeutung sein" entsprechen in keiner Weise dem Bestimmtheitsgebot und dem Verhältnismäßigkeitsgebot (nur eindeutig benannte, schwere Verbrechen sind auf diese Weise zu ahnden).

AK-Anliegen: Die Datenschutzbehörden sind für alle Datenschutzaspekte der Verordnung zuständig und als solche ausdrücklich zu nennen. Die Herausgabe von Verkehrsdaten (Punkt vii) ist mangels Konformität mit der Rechtsprechung des EuGH ersatzlos zu streichen.

Kontaktieren Sie uns!

In Wien:

Daniela Zimmer
T +43 (1) 501 65 12722
daniela.zimmer@akwien.at

Benedikta Rupprecht
T +43 (1) 501 65 12694
benedikta.rupprecht@akwien.at

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

www.arbeiterkammer.at

In Brüssel:

Florian Wukovitsch
T +32 (0) 2 230 62 54
florian.wukovitsch@akeuropa.eu

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.