AK EUROPA

Positionspapier
April 2022
Konstument:innen

COM(2022) 68

Datengesetz

Deutlich mehr Konsument:innenschutz fürs Internet der Dinge

Zusammenfassung

Worum geht es?

Der Verordnungsentwurf zielt darauf ab, Daten, die mit dem Internet verbundene Geräte erzeugen, vielen Beteiligten zugänglich zu machen – den Nutzer:innen der Produkte, dem sogenannten „Dateninhaber" (Hersteller:innen, Verkäufer:innen, Vermieter:innen oder sonstigen Berechtigten), berechtigten Dritten, öffentlichen Stellen und der Wissenschaft und Forschung im öffentlichen Interesse. Die Datenschutzgrundverordnung (DSGVO) und die e-Privacy-Richtlinie sollen dadurch nicht berührt werden.

Konsument:innen haben nach dem Datengesetz das Recht,

- über den Datenanfall informiert zu werden,
- auch selbst (möglichst direkten) Zugang zu diesen Daten zu erhalten und
- Dritten auf ihren Wunsch hin ebenfalls einen Datenzugriff zu verschaffen.

Zusammengefasste AK-Bewertung

Die Brisanz des Vorhabens wird sichtbar, sobald man die von der EU-Kommission vorgeschlagenen Regeln nicht nur auf visionäre Bereiche, wie autonom fahrende Autos oder Smart Homes anwendet. Aufgrund allgemeinster Formulierungen („wie die durch Nutzung des Produkts und verbundenen Dienstes erzeugten Daten genutzt werden") dürfte die VO auch für Millionen Alltagsgeräte und -dienste wie bspw digitale Fernsehgeräte, eBook-Reader, Sprachassistenten, Fitnesstracker uvm gelten. Konsument:innen laufen bei smarten Geräten (Internet der Dinge, IoT) Gefahr, wie beim Internetsurfen einer exzessiven kommerziellen Überwachung ihres Alltagsverhaltens, Profilbildungen und Verhaltensmanipulationen (durch gezielte Angebote, Werbung, personalisierte Preise) ausgesetzt zu sein. Unsere Privatsphäre gerät damit auch beim vernetzten Autofahren, Zähneputzen, Heizen, Sport Ausüben, Fernsehen, Spielen, unter Druck. Die digitale Souveränität der Verbraucher:innen über die bei der Geräte- und Dienstnutzung erzeugten Daten muss deshalb unbedingt gestärkt werden!

Denn: Was bliebe noch privat, wenn Fernseher und Saugroboter permanent Nutzungsdaten absaugen und Dritte genau wissen, wann bzw was sich X ansieht, wo und wann er/sie daheim und wie groß die Wohnung ist?

Interessen der Datenökonomie haben eklatanten Vorrang vor der digitalen Souveränität der Konsument:innen. Die EU-Kommission verfolgt mit ihrem Datengesetz das Ziel „eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft zu gewährleisten und den Datenzugang zu fördern". Dem von der EU-Kommission selbst gewählten Anspruch die „Nutzung von Daten [zu] kanalisieren und gleichzeitig hohe ethische, Datenschutz- und Sicherheitsstandards [zu] wahren" wird das Datengesetz nicht gerecht. Denn es beschäftigt sich über weite Strecken nicht mit diesen für Konsument:innen so wichtigen Schutzgütern, sondern vorrangig mit dem Schutz von KMUs und nichtdiskriminierenden Zugangsbedingungen dritter Parteien zu den Daten.

Das AK-Positionspapier zum Internet der Dinge hat schon vor Jahren auf die Gefahr einer Erosion der Verbraucher:innen(grund)rechte bei vernetzten Gütern aufmerksam gemacht und Schutzmaßnahmen empfohlen. Die AK hält angesichts der gesamtgesellschaftlichen Tragweite das Datengesetzes einen weitgehenden Schritt zurück an den Start für angemessen, um Verabsäumtes nachzuholen: Fachwissen aus dem Bereich des Verbraucher:innen- und Datenschutzes (EDPD, EDPS, BEUC, Zivilrechtsinstitute der Universitäten) sollte von Beginn an in die Ausarbeitung einbezogen werden, um Rechte und Pflichten der Beteiligten besser auszubalancieren. Zu den wesentlichsten Anliegen zählt:

- Digitale Selbstbestimmung von Verbraucher:innen/Bürger:innen
- Offline-Rechtsanspruch

Die Position der AK

Zum Hintergrund

Überwachungsrisiken

E-Book-Reader und vernetzte TV-Geräte senden Daten zum Nutzer:innenverhalten an Unternehmen, Fitnessarmbänder messen den Puls und liefern Gesundheitsdaten an Dritte, Fernsteuerungen im Smart Home heizen das Backrohr vor und Überwachungsboxen im Auto übertragen das Fahrverhalten an Versicherungen, die die Höhe der Prämienzahlung von den gemessenen Daten abhängig machen. Gegenstände, die ins Internet integriert sind, erlauben Firmen noch tiefere Einblicke in unser Leben – das Erstellen von Persönlichkeitsprofilen oder Prognosen über künftiges Verhalten inbegriffen. Da hilft es auch nicht, dass Art 6 die Datennutzungen von den Nutzer:innen beauftragte Dritte einschränkt (Profilingverbot). Die Vorschriften gelten nicht für den/die Dateninhaber:in und von ihm/ihr beauftragte Dritte.

Datenschutz

Der Entwurf zu einem Datengesetz räumt verschiedenen Beteiligten Daten-Nutzungsrechte ein. Zwischen personenbezogenen und nicht personenbezogenen Daten wird nicht unterschieden – ein Kardinalfehler. Angesichts völlig unterschiedlicher Rechtsfolgen ist es nicht sachgerecht, allgemein von Daten zu reden. Nur bei Daten ohne jeglichen Personenbezug kann die EU-Kommission Verbraucher:innen ein bloßes Mitspracherecht einräumen.

Deren Ansage „Wir wollen Verbrauchern und Unternehmen noch mehr Mitspracherecht darüber einräumen, was mit ihren Daten geschehen darf, indem klargestellt wird, wer zu welchen Bedingungen Zugang zu den Daten hat.“, ist vor dem Hintergrund, dass für die meisten Daten Verarbeitungseinschränkungen oder -verbote gelten, geradezu irreführend.

Geschäftsmodelle

Vernetzte Produkte weisen eine starke Servicekomponente auf. Statt einem klassischen Kauf mit vollständigem Eigentumsübergang (auch hinsichtlich digitaler Komponenten) werden wie bei urheberrechtlich geschützten Werken nur mehr Nutzungsrechte eingeräumt, die der/die Anbieter:in nach Gutdünken ausgestalten kann. Gegen das sich abzeichnende Ungleichgewicht von Rechten und Pflichten der Vertragspartner:innen besteht gesetzlicher Handlungsbedarf, dem der Entwurf nicht nachkommt (Das Datengesetz verbietet nur unfaire Vertragsklauseln zum Schutz von KMU). Eigentümer:innen können Dritte vom Zugriff auf ihr Eigentum ausschließen. Sind sie nur mehr Lizenznutzer:innen, kann ihnen die Datenökonomie Onlinezwang und Überwachungsmethoden einseitig diktieren. Konsument:innen entscheiden dann nicht mehr autonom, wie anonym sie Geräte nutzen. EG 20 erklärt, dass Nutzer:innen smarter Geräte „typischerweise eine Registrierung vornehmen müssen und einen individuellen Account erhalten“. Das Recht, Haushaltsgeräte weiterhin anonym nutzen zu können, muss gestärkt werden. Nutzer:innen unterliegen außerdem Kontrollen und Verboten, wenn sie die Sache verändern, selbst reparieren oder reparieren lassen wollen. Die Eigentümer:inneneigenschaft der Konsument:innen am gesamten Produkt müsste klargestellt werden.

Onlinezwang

Mit dem Internet der Dinge in Kinderspielzeugen sind Überwachungspraktiken auch in Kinderzimmern angekommen. Kleinstkinder konnten zB mit der Puppe Cayla erste Erfahrungen mit kommerziellen Vertraulichkeitsverletzungen sammeln. Über Bluetooth-Verbindung, Mikrofon und Spracherkennung konnten Unterhaltungen an den US-Hersteller weitergeleitet werden. Probleme, die mit Online-Spielen generell verbunden sind: verstecktes Aufzeichnen des Verhaltens und Intransparenz der Datenempfänger:innen und Datennutzungszwecke. Bei vielen Spielen besteht Onlinezwang, auch

dann, wenn ein Spiel alleine gespielt wird und eine Internetverbindung nicht erforderlich wäre. Dieser Druck zu einem „always-on" dürfte sich verstärken. Ohne ein explizit verankertes „Offline"-Recht werden Verbraucher:innen nur die Wahl haben: „take it – or leave it" (siehe AK Studie).

Zusammengefasst zeichnet sich ein krasses Ungleichgewicht in den Rechtspositionen zwischen den Anbieter:innen und ihren Kund:innen ab. Die Anbieter:innenseite,

- nützt vertragliche und technische Gestaltungsmöglichkeiten um personenbezogene Kund:innendaten und Betriebsdaten der Geräte zu analysieren und kommerziell zu verwerten;
- übernimmt wenig Verantwortung (Zusicherung von Qualitäten, Haftung bei Schäden, Gewährleistung bei Defekten) für IoT-immanente Risiken (Softwarefehler, Hackingangriffe, Databreaches, Insolvenzen mitbeteiligter Anbieter:innen, schädigender Einsatz unausgereifter Algorithmen und Künstlicher Intelligenz) und investiert nicht in präventive Sicherheit;
- schwächt Konsument:innen dadurch, dass mit einem Kauf verbundene Eigentumsrechte auf einzelne Komponenten bezogen immer öfter ausgehebelt und durch bloße urheberrechtliche Nutzungsrechte ersetzt werden;
- überwacht Verbraucher:innen, die sich durch einen dicht vernetzten Alltag bewegen. Jeder Berührungspunkt mit smarten Geräten hinterlässt persönliche Datenspuren, die in umfassenden Nutzungs- und Standortprofilen münden können. Die mit dem Tracking von PC- und Handynutzern begonnene Entwicklung der Überwachung der Alltagshandlungen erlangt mit IoT eine neue Dimension. Die Schnittstellen mit dem Internet, an denen Verbraucher:innenverhalten beobachtet, ausgewertet und Dritten übermittelt werden kann, verdichten sich und ergeben ein einzigartig genaues Bild über das, was wir tun, lassen, denken, mit wem wir in Kontakt stehen u.v.m.;
- setzt Verbraucher:innen Sicherheitsrisken aus: Im Wettlauf um innovative Produkte, die man rascher als die Konkurrenz auf den Markt bringt, landen völlig unausgereifte Geräte in Haushalten. Darüber hinaus gilt systembedingt, dass Software so gut wie nie völlig fehlerfrei sein kann. Sicherheitsupdates tragen diesem Umstand Rechnung. Was den Konsument:innen an Entwicklungsrisken, fehlender Marktreife und mangelnden präventiven Sicherheitsmaßnahmen gegen Schadsoftware, Databreaches und Hackingangriffen zugemutet werden kann bzw was nicht, befindet sich bestenfalls im Diskussionsstadium. Es besteht die Gefahr, dass Konsument:innen als „Versuchskaninchen" von aus technischer oder Datenschutz-Sicht unsicheren Produkten dienen. Oft wird erst reaktiv in Produkt- und Datensicherheit investiert, wenn Pannen mit erheblichen Auswirkungen (und Medienecho) bereits passiert sind.

Die AK sieht folgenden Verbesserungsbedarf

Digitale Selbstbestimmung von Verbraucher:innen/Bürger:innen

Fairnessregeln und Schlichtungsstellen sieht das Datengesetz nur für Konflikte zwischen den am Datenfluss beteiligten Unternehmen vor. Den Verbraucher:innenbedürfnissen und ihren Rechtsschutzinteressen widmet sich der Entwurf (mit Ausnahme eines Rechts auf Information, Datenzugriff und „Daten Teilen") nicht. Konsument:innen, die Produkte kaufen, werden im Entwurf als „Nutzer" (statt als Eigentümer:in mit alleinigen Verfügungsrechten) betrachtet. Konsument:innen haben kein abgesichertes Recht, ihr Produkt offline nutzen oder die Datengenerierung einschränken zu können. Sie genießen (im Gegensatz zu KMUs) keinen (über die RL 93/13/EG hinausgehenden) Schutz vor IoT-spezifischen, unfairen Vertragsbedingungen. Es ist unklar, ob sie ihr individualisiertes Produkt weiterverkaufen oder selbst reparieren können. Inakzeptabel ist auch, dass die Pflichten der Datenempfänger:innen nach Art 6 (zB keine Manipulation und Verhaltensprofile der Nutzer:innen) nicht für den/die Dateninhaber:in gelten.

Offline-Rechtsanspruch

Nutzer:innen haben ein starkes Interesse daran, vernetzte Funktionen wahlweise abzuschalten und die Hauptfunktionen des Produktes trotzdem offline nutzen zu können. Hersteller:innen und Dienstanbieter:innen haben gegenläufige Interessen (know your customer, mehr Gewinn durch vernetzte Zusatzservices, Datenverkauf). Somit muss das Recht, Internetverbindungen – ohne Verlust von Kernfunktionen des Gerätes – deaktivieren zu können, rechtlich abgesichert werden. Welchen hohen Stellenwert dieses Offline-Recht hat, zeigt das Beharren vieler Konsument:innen auf einer Abschaltfunktion bei Smart Meter, den digitalen Stromzählern.

Schlüssiger Anwendungsbereich

Haushaltsgeräte, Konsumgüter und virtuelle Assistenten sind erfasst (EG14 und 22), „Geräte, die primär zum Abspielen von Inhalten bestimmt sind, wie zB PCs, Server, Handys, Kameras", aber nicht. Weshalb Siri, Alexa und mutmaßlich auch smarte TV-Geräte, die ebenso Lieferant:innen von Inhalten sind, in das Datengesetz aufgenommen werden, Smartphones aber nicht, wirkt äußerst willkürlich. Letztere sollten jedenfalls in den Anwendungsbereich fallen.

Rollen und Verantwortlichkeiten klären

Wer unter mehreren möglichen Beteiligten (Hersteller:innen, Zusatzdienstanbieter:innen, Softwarelieferant:innen, Verkäufer:innen, andere Dritte) der/die sogenannte Dateninhaber:in ist, geht aus dem Entwurf nicht klar hervor. Aus welchen EU-Vorschriften sich definitionsgemäß die Rolle der/des Dateninhaber:in zweifelsfrei ableiten lässt und welche Ermächtigungen damit verbunden sind, ist ungeklärt. Ebenso die Frage, wer welche Pflichten gegenüber den Konsument:innen zu erfüllen hat. Rollen und damit verbundene Verantwortungen sind im Entwurf klar und rechtssicher zu benennen.

Personenbezug klarstellen

Das Datengesetz bezieht sich gleichermaßen auf personenbezogene Daten wie Daten ohne Personenbezug. Dass die Vorschriften nicht zwischen den Datenarten unterscheiden, ist ein konzeptioneller Fehler. Was in einem Fall harmlos sein mag, kann im anderen eine schwerwiegende Grundrechtsverletzung darstellen. Nicht wenige Wissenschaftler:innen meinen im Übrigen, dass Gerätedaten nahezu immer einen grundrechtlich geschützten (mittelbaren) Personenbezug aufweisen. Unterschiedslos von „Daten" zu reden, kann somit Kalkül sein: die Datenökonomie wird sich in der Praxis oft unreflektiert auf Nutzungsrechte berufen, denen die DSGVO entgegensteht. Bereits jetzt weit über ihre Grenzen geforderte Datenschutzbehörden können dies nicht annähernd regelmäßig prüfen. Da hilft es auch nicht, dass nach EG 5 nicht beabsichtigt ist, mit der VO neue Rechtsgrundlagen für die Datenverarbeitung zu schaffen. Bei sonstigen Daten mag ein Informations-, Zugriffs- und „Daten Teilen"-Recht reichen. Nach der DSGVO sind hingegen Prinzipien wie Datensparsamkeit zu beachten und Datennutzungen ohne Rechtsgrundlage verboten. Die EUGH-Rechtsprechung zur DSGVO kommt nur äußerst schleppend voran. Die Datenökonomie profitiert von der Rechtsunsicherheit, ob im Einzelfall Personenbezug besteht oder nicht.

Grundrechtliche Balance bei Datenzugriffen in Notfällen

Auch mit Grundrechtsschranken hält sich der Entwurf nicht lange auf: öffentliche Stellen, aber auch ominöse (weil undefinierte) Agenturen und Einrichtungen, können Daten anfordern, wenn bei der Erfüllung öffentlicher Interessen in einem Notfall ein nicht näher definierter „außerordentlicher Bedarf" besteht. Eisbrecher zugunsten der Analyse von Bevölkerungsdaten ist zweifellos die Massenauswertung von Daten der Mobilfunkbetreiber:innen zur besseren Bewältigung der aktuellen Pandemie. Die Eingriffserlaubnis des Datengesetzes in die Privatsphäre der Bürger:innen ist aber derart unbestimmt, dass auch im Falle wenig gewichtiger öffentlicher Interessen und Notfälle auf sensible Gerätedaten zugegriffen werden könnte.

Keine Schutzlücken durch Ausnahmen für KMUs, die das Recht der Konsument:innen auf Information, Zugriff und „Sharing" von Daten dem Entwurf zufolge nicht beachten müssten.

Mit Blick auf das Vertragsrecht müssen Konsument:innen außerdem…

- in jeder Hinsicht autonom über das gekaufte Produkt verfügen können;
- Eigentum am Produkt mit allen eingebauten Softwarekomponenten haben;
- ein uneingeschränktes Selbstbestimmungsrecht über alle Daten haben, die das Produkt erzeugt;
- ohne jeden Zwang darüber entscheiden können, ob und wem sie diese Daten zugänglich machen;
- ihre Werkstätten und Serviceanbieter:innen in jeder Hinsicht frei wählen dürfen und nicht gezwungen sein, Koppelungsverträge zu akzeptieren;
- darauf vertrauen dürfen, dass der Hersteller:in/ Verkäufer:in sich nicht auf Haftungs- und Gewährleistungsausschlüsse berufen kann, wenn der/die Verbraucher:in sich seine/ihre Werkstätte frei aussucht oder nicht alle anfallenden Daten zugänglich macht
- Geräte auch selbst reparieren dürfen und
- ein Wahlrecht haben (Produkte müssen deaktivierbare smarte Funktionen haben).

Zu den Details des Kommissionsentwurfs

Art 1

Der Vollharmonisierungscharakter schadet der Rechtssicherheit. Wie andere grundrechtsrelevante VO (DSGVO, DGA) sind die Bestimmungen zu allgemein gehalten, um komplexe Sachverhalte rechtssicher zu regeln. Es bedarf sektorspezifischer Präzisierungen, damit Normadressat:innen nicht vor unzähligen, gerichtlich zu klärenden Auslegungsfragen stehen. Da der Entwurf auch öffentlichen Stellen (bzw nicht näher definierten Agenturen oder Einrichtungen, die im öffentlichen Interesse handeln), Rechte und Pflichten einräumt, muss daran erinnert werden, dass diese entsprechend dem österr. Art 18 B-VG (Legalitäts- und Bestimmtheitsgebot) nur kraft ausreichend determinierter Gesetze tätig werden.

Der Anwendungsbereich bezieht sich sowohl auf personenbezogene Daten nach der DSGVO als auch solche ohne Personenbezug. Ein konzeptioneller Fehler: eine Trennung ist vorzunehmen und anhand von Kriterien zu bestimmen, wann ein Personenbezug als gegeben gilt. One-size-fits-all-Regeln werden den unterschiedlichen Bedürfnissen der geschützten Personen (Konsument:innen als data subjects oder Unternehmen als Inhaber:innen geistiger Eigentumsrechte) und unterschiedlichen Risiken nicht gerecht.

Art 2

Die Definition „Dateninhaber" ist viel zu unscharf: Dateninhaber:in wäre jede/r, der/die das Recht oder die Pflicht hat (aufgrund des Datengesetzes oder sonstigem EU-Recht) bestimmte Daten zugänglich zu machen. Die vage Definition lässt offen, wer nun genau Konsument:innen zu informieren hat bzw. auf Zugriffs- bzw Datenteilungswünsche reagieren muss.

Der Begriff „Dateninhaber" ist auch unpassend: an unveräußerlichen Persönlichkeitsrechten bestehen keine Besitz- oder Eigentumsrechte. Diesem Umstand trägt die DSGVO auch dadurch Rechnung, dass Zustimmungen zur Datennutzung stets widerrufbar sein müssen. Insofern wäre es zutreffender, von Verantwortlichen nach der DSGVO zu sprechen, die personenbezogene Daten unter Einhaltung der Art 5 ff DSGVO nützen dürfen und Rechteinhaber:innen an sonstigen, nicht personenbezogenen Daten aufgrund entsprechender Vereinbarungen oder gesetzlicher Vorschriften. Diese Unterscheidung müsste den gesamten Entwurf durchziehen, tut es aber – zum Nachteil für Rechtssicherheit und Konsument:innen – nicht.

Die Definition „Nutzer" schwächt die Position von Käufer:innen: Nutzer:in soll sein, wer ein Produkt besitzt, mietet oder least. Welche Rechtsposition diese Person in Bezug auf (nicht) personenbezogene Daten hat, ist unklar und dringend regelungsbedürftig. Eigentümer:innen können frei entscheiden, etwa Produkte offline zu nutzen, Dritte vom Zugriff auf Produkte auszuschließen etc. Ein Nutzungsrecht ist kein dem Eigentum vergleichbares Verfügungsrecht!

Art 3

Pflichtenadressat:innen klären: Der Entwurf vermeidet es durchgehend, die Pflichtenadressat:innen zu benennen. „Produkte werden so konzipiert" dürfte sich an den/die Hersteller:in richten. Wer aber hat die folgende Vorschrift umzusetzen: „Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein Produkt oder verbundenen Dienst werden dem/der Nutzer:in mindestens folgende Informationen in einem klaren und verständlichen Format bereitgestellt"? Diese Unschärfe ist deshalb inakzeptabel, weil auch die Definition des/der Dateninhaber:in Raum für Spekulationen lässt. Wenn die Rolle des/der Dateninhaber:in sich aus dem EU-Recht ergeben soll, sollten Konsument:innen auch erfahren, aus welchen Rechtsvorschriften sich das im Einzelfall erschließt. Nach Art 3 Abs 2 lit e kann der/die Dateninhaber:in jedenfalls „Verkäufer, Mieter oder Leasinggeber" oder auch jemand ganz anderer sein (naheliegend wäre der/die Hersteller:in des Produktes). Art 3 Abs 2 lit d verpflichtet (wen auch immer) dazu, klarzustellen, ob der/die Herstellerin, der das Produkt unterstützt oder der/die Anbieter:in von Zusatzdiensten beabsichtigen, Daten selbst zu nutzen oder Dritten dies zu erlauben. Diese Gemengelage unklarer Rollen und Verantwortlichkeiten ist gründlich zu überarbeiten.

Die Bestimmung enthält einige zweckmäßige Infopflichten gegenüber Verbraucher:innen. Sie sollte aber ergänzt werden um...

- Anleitungen, wie die Datengenerierung eingeschränkt bzw. deaktiviert werden kann.
- Informationen, welche unabhängige Schlichtungsstelle Konsument:innen anrufen können, um Fragen/Beschwerden über die rechtskonforme Umsetzung der VO zu klären und ihre Rechte durchzusetzen.
- die Vorgabe, dass die Infopflichten nach Art 3 gut sichtbar und gemeinsam mit jenen der DSGVO (Art 12 bis 14) zu erfüllen sind. Die Informationen müssen sich auch auf Produktverpackungen finden.

Nachbesserung der "By Default"-Pflicht: Begrüßt wird, dass die Bestimmung proprietäre / in sich geschlossene Systeme praktisch verbietet. Um

Daten-Teilen mit Dritten zu ermöglichen, sind offene Standards nötig. Unklar ist aber, wie der „By Default" – Grundsatz bei der Herstellung von Produkten konkret umzusetzen ist. Der Bestimmung zufolge soll das Produktdesign dem/der Produktnutzer:in einen leichten Datenzugang verschaffen. Es sind zumindest Beispiele zu nennen, was genau von dieser Pflicht umfasst ist. Da „By Default" idR verbraucherfreundliche Voreinstellungen meint, sollte klargestellt werden, ob und welche Auswahloptionen Konsument:innen vorfinden müssen. Kernforderungen der AK sind, dass

- Produkte „by design" so zu konstruieren sind, dass sie auf einfache Weise wahlweise auch offline nutzbar sind.
- Produkte für Käufer:innen gut sichtbar gekennzeichnet sind, wenn ihre Nutzung aufgrund technisch zwingender Erfordernisse für ihren grundlegenden Gebrauch Onlineverbindungen voraussetzt.
- ein Verbot eines zwingenden "Always-On" verankert wird: außerhalb der Betriebszeiten müssen Verbraucher:innen die Internetanbindung und Datengenerierung auch bei nur online nutzbaren Produkten (entgegen EG 17) leicht deaktivieren können.
- auch nicht-personenbezogene Daten (in Analogie zur DSGVO) datensparsam über Einstellungen geregelt werden können. Dies nicht zuletzt deshalb, weil die Frage, wann ein mittelbarer Personenbezug vorliegt, höchst umstritten ist. Im Zweifel muss der/die Käufer:in eines Produktes jeden für die Basisnutzung eines Produktes nicht nötigen Datenfluss unterbinden können.

Art 4

Direktes Zugangsrecht des Nutzers zu den Daten: Die Bestimmung sieht Auskunftsrechte der Nutzer:innen vor, sollten die Daten nicht direkt zugänglich sein. Art 3 sieht dem gegenüber vor, dass die Daten Nutzer:innen „leicht, sicher, und wo relevant und geeignet, direkt zugänglich sein müssen." Es erhellt sich nicht, wann der direkte Datenzugang nicht „relevant und geeignet" ist. Wenn Betriebsdaten leicht erzeugt und auch verwertet werden können, ist es den Hersteller:innen und Softwarelieferant:innen grundsätzlich auch zumutbar, eine Schnittstelle für einen direkten Datenzugang der Konsument:innen einzurichten. Wo es technisch unmöglich ist oder kostenseitig unverhältnismäßig, sollte die VO näher erläutern und Aufsichtsbehörden zu einem entsprechenden Marktmonitoring verpflichten.

Nachweis im Einklang mit der DSGVO: Bei personenbezogenen Daten ist darauf hinzuweisen, dass den Informationspflichten nach Art 13-14 DSGVO nachzukommen ist, ohne dass der/die Betroffene sich zuvor identifizieren müsste. Nur beim Auskunftsrecht nach Art 15 kann unter Umständen eine Klärung der Betroffeneneigenschaft nötig sein. In Art 4 muss deshalb unbedingt zwischen (nicht) personenbezogenen Daten unterschieden werden.

Vorrang von Transparenz vor Geschäftsgeheimnissen: Käufer:innen brauchen aussagekräftige Informationen vor dem Kauf (um sich in Kenntnis der Tragweite für oder gegen ein Produkt entscheiden zu können) und während des Gebrauchs (um den Datenfluss kontrollieren und bei Bedarf ändern zu können). Geschäftsgeheimnisse dürfen dem Transparenzbedürfnis nicht entgegenstehen.

Art 5

Faire Verträge zwischen „Dateninhabern" und „Nutzer": Während sich etliche Bestimmungen dem Kräfteungleichgewicht im B2B-Sektor und unlauteren B2B-Geschäftsbedingungen widmen, fehlt dies in Bezug auf Verbraucher:innen vollständig. Es wird lediglich normiert, dass nicht-personenbezogene Daten nur auf Basis vertraglicher Übereinkünfte genutzt werden dürfen. Der/die Dateninhaber:in darf die Daten nicht dafür nutzen, Einblicke in die ökonomische Situation, Produktionsweise oder gewerbliche Datennutzung eines/r Nutzer:in zu bekommen. Schutzadressat:innen sind kommerzielle Nutzer:innen, die ein Ausspionieren ihrer betrieblichen Situation befürchten. Wo bleiben die Schutzmaßnahmen für Nutzer:innen, die Konsument:innen sind? Auf ihren Schutzbedarf bei unfairen Verträgen zu vergessen, ist inakzeptabel.

Art 6

Viele Betriebsdaten unterliegen der DSGVO. Es braucht deshalb eine sektorspezifische RL für den Umgang mit personenbezogenen Daten bei IoT-Produkten. Die DSGVO ist zu allgemein um Auskunft darüber zu geben, wann Dritte (aber auch der/die völlig unregulierte Dateninhaber:in) Nutzer:innendaten speichern und für verschiedene Zwecke verwenden dürfen. Wann ist eine Zustimmung erforderlich? Wann können berechtigte Interessen geltend gemacht werden? Welche Sicherheitsmaßnahmen sind erforderlich? Diese Fragen klärt die VO nicht und auch die DSGVO kennt hierzu keine Antworten. Es ist Verbraucher:innen nicht zumutbar, bei elementaren Fragen zu IoT-Produkten jahrelang auf Gerichts- bzw Behördenentscheidungen warten zu müssen. Außerdem sehen wir, dass die Mitgliedstaaten in Einzelfällen völlig heterogene Antworten auf Auslegungsfragen der DSGVO geben. Vor diesem Hintergrund ist eine IoT-Datenschutz RL zum Schutz

vor Rechtsunsicherheiten und überschießenden Datenverwendungen erforderlich.
Die Anforderungen an Dritte (zB "Verbot von dark patterns" oder für die Diensterbringung nicht erforderliches Profiling) werden begrüßt, sollten aber unbedingt auch für den/die Dateninhaber:in gelten. Es ist nicht akzeptabel, dass diese/r nicht dieselben Fairness-Regeln einhalten muss.

Art 7

Unsachliche Entbindung von KMUs von den Pflichten im Kapitel 2: Egal ob klein oder groß: die Regeln für die Verwertung von Daten müssen auf Transparenz, Fairness und elementaren Grundrechtsschutz abzielen und sind von jedem/r Wirtschaftsteilnehmer:in einzuhalten. Die Ausnahme ist sachlich unbegründet, setzt Verbraucher:innen unnötig Risiken aus bzw verschlechtert ihre Rechtsposition und informationelle Lage. Vor diesem Hintergrund sollte Art 7 gestrichen werden.

Art 10

Streitschlichtung nicht nur bei B2B-Konflikten: Dateninhaber:in und Daten-Empfänger:in können ihre Konflikte vor einer unabhängigen Streitschlichtungsstelle austragen. Ein solches, niedrigschwelliges System sollte auch Konsument:innen offenstehen. Es zählt zu den schwer nachvollziehbaren Defiziten des Entwurfes, nur B:B-Konflikte zu berücksichtigen.

Art 11

Sanktionen fehlen: Den unauthorisierten Zugang zu Daten zu beenden und die unzulässig gespeicherten Daten zu löschen, kann nicht ernsthaft die einzige Folge von Datenmissbrauch sein. Da die VO – wie mehrfach betont – nicht zwischen (nicht) personenbezogenen Daten unterscheidet, ist auf die DSGVO hinzuweisen (ua data breach notification, Sanktionen). Ähnliche Maßnahmen sollten für – oft auch nur vermeintlich – nicht-personenbezogene Daten gelten, um Missbrauchsfälle durch einigermaßen abschreckende Sanktionen gering zu halten. Die Ausnahmebestimmungen stellen nur auf die Situation des/der Dateninhaber:in ab (kein signifikanter Schaden, Unverhältnismäßigkeit) und vergessen abermals die mindestens ebenso betroffenen Verbraucher:innen.

Art 13

Unfaire AGBs gegenüber KMUs: Es gibt (außer den Vorgaben der RL 93/13/EG) keine Schutzbestimmungen im Verbraucher:innenrecht, die spezifisch auf die Vertragsrisiken von IoT abstellen. Dass KMUs als schutzwürdig angesehen werden, Verbraucher:innen aber nicht, ist sachlich nicht nachvollziehbar.

Kapitel 5

Zugriff von öffentlichen Stellen unter Umständen nicht grundrechtskonform: Die Bestimmungen des Kapitels sind zu vage, um eine unmittelbare rechtliche Grundlage für das Handeln von Behörden darzustellen, die nur aufgrund präzise formulierter gesetzlicher Anordnungen tätig werden dürfen. Sollten die Bestimmungen nur auf die Herausgabepflichten der Dateninhaber:innen abzielen, müsste explizit darauf hingewiesen werden, dass diese nur dann gelten, wenn im nationalen oder EU-Recht eine hinreichend konkrete behördliche Ermächtigung verankert ist. Zu den Unzulänglichkeiten des Kapitels zählt:

- Nicht nur öffentliche Stellen, sondern auch „Agenturen und Einrichtungen, die im öffentlichen Interesse handeln" können „bei außergewöhnlichem Bedarf" (Ausnahme sicherheitspolizeiliche Aufgaben) personenbezogene Daten herausverlangen. Die elementaren Voraussetzungen an eine einigermaßen rechtssichere Norm sind nicht erfüllt. Wer, was, wann, wie darf, bleibt im hohen Maß unklar. Die berechtigten Agenturen und Einrichtungen werden nicht näher definiert. Welcher Bedarf muss vorliegen, damit in die verfassungsrechtlich geschützten Rechte auf Datenschutz und Privatsphäre eingegriffen werden darf?

- Die Tragweite dieser Bestimmung ist jedenfalls enorm. Jedes smarte Auto unterliegt dem Anwendungsbereich der VO, womit auch alle personenbezogenen Standortdaten von öffentlichen Stellen, die einen besonderen Bedarf behaupten, ausgewertet werden könnten. Ohne gerichtliche Anordnung kann aber nicht ernsthaft auf Millionen Nutzer:innendaten zugegriffen werden. Art 17 normiert zwar, dass – soweit als möglich – nicht personenbezogene Daten angefordert werden sollen und Art 18, dass „vernünftige Anstrengungen unternommen werden sollen, die angeforderten Daten zu pseudonymisieren". Letzteres aber auch nur, wenn der Zweck der Abfrage mit pseudonymisierten Daten erfüllt werden kann.

Aufgrund seiner unverhältnismäßigen Eingriffstiefe in die Grundrechte der Bevölkerung muss das Kapitel unter Zuziehung des EU-Datenschutzbeauftragten und EU-Datenschutzausschusses gründlich überarbeitet werden.

Kontaktieren Sie uns!

In Wien:

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

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

www.arbeiterkammer.at

In Brüssel:

Alice Wagner
T +32 (2) 230 62 54
alice.wagner@akeuropa.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.