AK EUROPA

Positionspapier
April 2020
KonsumentInnen

Evaluation der Datenschutz-Grundverordnung (DSGVO)

Zusammenfassung

Bis 25.05.2020 hat die EU-Kommission dem EU-Parlament und Rat einen Bericht über die Bewertung und Überprüfung der DSGVO vor (Art 97 DSGVO) vorzulegen. Erforderlichenfalls schlägt sie Änderungen der Verordnung vor. Dabei berücksichtigt sie die zwischenzeitigen technischen Entwicklungen. Im Interesse der betroffenen KonsumentInnen und ArbeitnehmerInnen sind folgende Verbesserungen notwendig, damit das Grundrecht auf Datenschutz durch eine Überarbeitung der DSGVO wirklich den Stellenwert bekommt, den es verdient:

Die DSGVO hat für KonsumentInnen bzw ArbeitnehmerInnen einige Verbesserungen gebracht (zB strengere Anforderungen an Zustimmungen, Einbeziehung von Verantwortlichen aus Drittstaaten, abschreckende Sanktionen). Insgesamt hat sich die Rechtsposition der KonsumentInnen und ArbeitnehmerInnen aber nicht entscheidend verbessert. Viele der im Folgenden beschriebenen Anliegen von KonsumentInnen bzw ArbeitnehmerInnen sind in der Praxis nach wie vor nicht erfüllt. Die Gründe dafür sehen wir in Vollzugsdefiziten aber vor allem auch in Unzulänglichkeiten der DSGVO selbst.

In Punkt 1 beschreiben wir die Ausgangslage: Die DSGVO löst den Interessenskonflikt zwischen zentralen Datenschutzbedürfnissen von KonsumentInnen bzw ArbeitnehmerInnen und den Trends in der Datenökonomie unzureichend.

In Punkt 2 gehen wir auf praktische Probleme bei der Anwendung der DSGVO im Alltag der KonsumentInnen bzw ArbeitnehmerInnen ein und schlagen in Punkt 3 konkrete Änderungen in der Verordnung vor.

In Punkt 4 fassen wir unsere Erfahrungen mit Hindernissen bei der Rechtsdurchsetzung zusammen und schlagen in Punkt 5 Verbesserungen vor.

In Punkt 6 verweisen wir schließlich auf Trends, wie das Internet der Dinge und den Einsatz von Algorithmen, deren Herausforderungen für den Datenschutz trotz DSGVO weitgehend ungelöst sind.

Die Position der AK

1. Ausgangslage

Verbot mit Erlaubnisvorbehalt nach der EU-Menschenrechtscharta

Nach Art 8 der EU-Grundrechtscharta hat jede Person Anspruch auf Geheimhaltung seiner Daten, soweit ein schutzwürdiges Interesse daran besteht. Beschränkungen des Anspruchs sind nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig. Aber selbst dann darf nur in der gelindesten Form ins Grundrecht eingegriffen werden. In der Praxis erhält das Grundrecht aber oft nicht den Stellenwert, der ihm gebührt.

Unser Bewertungsmaßstab

Eine Eurobarometerumfrage aus 2015 ergab folgende zentrale VerbraucherInnenanliegen: 92 % der Befragten wünschten sich einen Vorrang des Datenschutzes gegenüber wirtschaftlichen Interessen. 78 % meinten, OnlineanbieterInnen besäßen viel zu viele KundInnendaten und 73 % wollten immer um ihre ausdrückliche Zustimmung zur Datennutzung gefragt werden.

Erfüllt die DSGVO die Hoffnung der überwältigenden Mehrheit der VerbraucherInnen?

Entscheiden KonsumentInnen aktuell selbstbestimmter über ihre Daten? Wurde dem Anliegen von zwei Drittel der Befragten, immer nach ihrer Zustimmung gefragt werden zu wollen, entsprochen? Die Marktentwicklung der letzten 5 Jahre geht in Richtung einer Datenökonomie, die nach immer mehr Daten für immer mehr Zwecke verlangt. Es spricht daher einiges dagegen, dass sich die Lage für die KonsumentInnen maßgeblich verbessert hat.

EU-weite Förderung datengetriebener Wirtschaft

Politik, Wirtschaft und Forschung stellen aktuell die Weichen für den Übergang zu einer datengesteuerten Wirtschaft und zur Freisetzung des wirtschaftlichen Potenzials von Daten innerhalb der EU (siehe ua das Weißbuch zu künstlicher Intelligenz COM (2020) 65 oder die Mitteilungen COM (2020) 66 über eine europäische Datenwirtschaft oder COM (2018) 283 über den Weg zur automatisierten Mobilität. Angesprochen sind dabei Daten mit und ohne Personenbezug und solche, bei denen der Personenbezug entfernt wurde, die also anonymisiert wurden. Bezüglich letzterer Kategorie räumen ExpertInnen ein, dass Algorithmen durch fortschreitendes maschinelles Lernen so gut wie jede Anonymisierung rückführen können. Mit anderen Worten: KonsumentInnen werden re-identifizierbar. Wann Daten als nicht rückführbar anonymisiert gelten, ist gesetzlich nicht geregelt.

„Making more data available"...

...lautet die Devise. Der europäische Weg sei es „den Austausch und die breite Nutzung von Daten zu kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethikstandards zu wahren". Der Entwicklung zu einer Datenökonomie steht bei personenbezogenen oder nicht verlässlich anonymisierten Daten der Grundsatz der Datensparsamkeit entgegen. Der Bedarf von künstlicher Intelligenz nach immer mehr Trainingsdaten für die Suche nach unbekannten Mustern und Zusammenhängen ist auch mit den Geboten der Zweckbindung und von privacy by design bzw default oft nicht in Einklang zu bringen. In Aussicht gestellt wird ein in der Realität oft nicht einlösbares „sowohl als auch" von Datenökonomie und Grundrechten.

Gebraucht wird ein ehrliches Bekenntnis, dass manchmal auch nur eine „entweder oder"-Option besteht: Wissenschaftliche und kommerzielle Ausbeutung von großen Datenpools für unbestimmte Zwecke oder ein hohes Datenschutzniveau.

2. Praktische Probleme bei der Anwendung der DSGVO im Alltag

Defizite im Alltag der KonsumentInnen: Aufgrund vieler Beratungsanfragen wissen wir, dass

- KonsumentInnen mit überlangen, nichtssagenden Datenschutz- und -nutzungserklärungen konfrontiert sind.
- sie sich mit unübersichtlichen, dem Selbstbestimmungsrecht nicht entsprechenden technischen Datenschutzeinstellungen plagen.
- sie sich bei Auskunftsbegehren mit unpräzisen Antworten und dem Zweifel, herumschlagen, ob die Antworten richtig und vollständig sind.
- sich AnbieterInnen immer öfter damit rechtfertigen, dass eine Datenverarbeitung keiner Zustimmung bedarf, weil sie im – schwer überprüfbaren – überwiegenden berechtigten Interesse des Unternehmens oder Dritter erfolgt.
- die Rechtsgrundlage (überwiegender) berechtigter Nutzungsinteressen an Daten KonsumentInnen strukturell benachteiligt. Obwohl die Beweislast bei den DatennutzerInnen liegt, sind sie es, die in der Praxis nachweisen müssen, dass ihre Geheimhaltungsinteressen überwiegen. Eine Einigung mit den DatennutzerInnen ist völlig unrealistisch. Damit müssten KonsumentInnen in jedem Einzelfall Datenschutzbehörden oder Gerichte um deren Interessensabwägung ersuchen. Angesichts des Aufwands bleiben Rechte ungenützt und Rechtswidrigkeiten bestimmen weiterhin den Geschäftsalltag.
- ihnen der Einblick in algorithmische Entscheidungsprozesse mit der Begründung vorenthalten wird, die Entscheidung erfolge nicht „ausschließlich“ sondern „nur“ teilweise automatisiert oder die Bewertung sei nicht mit rechtlichen oder „erheblich“ beeinträchtigenden Folgen für die VerbraucherInnen verbunden. KonsumentInnen beklagen in Bezug auf den Einsatz von Algorithmen somit weiterhin nicht vertrauenserweckende Intransparenz.
- Daten jahrelang gespeichert werden. Dabei können KonsumentInnen (oder die Datenschutzbehörden) den im Einzelfall angemessenen Zeitraum oft nicht abschätzen. Sie haben keinen Einblick in die Betriebsabläufe. Wie lange Daten “erforderlich“ sind, ist häufig ein Werturteil und nicht objektiv festzustellen.
- so gut wie nie die genauen EmpfängerInnen ihrer Daten beauskunftet werden, sondern nur die „Empfängerkreise“, weil Unternehmen aus der DSGVO ein Wahlrecht ableiten.
- so gut wie nie Auskunft über die Herkunft der Daten erteilt wird, weil Unternehmen nur „verfügbare“ Informationen beauskunften müssen und Informationen daher praktisch nie verfügbar sind.
- ihr Wunsch nach physischer Löschung ihrer Daten nicht durchgesetzt werden kann. Sie müssen sich mangels klargestelltem Rechtsanspruch oft mit einer Anonymisierung ihrer Daten zufriedengeben. Ob und wie verlässlich anonymisiert wird, löst bei den KonsumentInnen berechtigtes Misstrauen aus.
- sie sich mangels einzuhaltender Standards und Nachweise nie darauf verlassen können, dass eine Rückführbarkeit anonymisierter Daten auf ihre Person ausgeschlossen ist.
- sie sich bei behaupteter Löschung mangels für sie sichtbarer Nachweise nur selten darauf verlassen können.
- sie die Identifikationspflichten oft von der Ausübung ihres Auskunftsrechtes abschrecken, zB wenn sie sich unseriösen Internetanbietern gegenüber ausweisen müssen.
- sie sich als Auskunftssuchende auch in Fällen identifizieren müssen, in denen DatennutzerInnen bei der Onlineregistrierung ihre Identität nicht abgeklärt hat.
- sie mit der Weitergabe von Daten (zB Standortdaten) für wissenschaftliche Zwecke in pseudonymisierter oder anonymisierter Form oft nicht einverstanden sind. Sie vermissen ein Einwilligungsrecht und sind verärgert, wenn ihnen nur Widerrufsrechte eingeräumt oder gar überwiegende berechtigte Interessen entgegengehalten werden.
- algorithmische Entscheidungen über Bonität und Zahlungsausfallswahrscheinlichkeiten von KonsumentInnen getroffen werden, ohne dass der massive Grundrechtseingriff auf Fälle mit hohen Ausfallsrisiken (Kredite, Ratenzahlung) beschränkt wäre. Bewertet wird inzwischen bei den geringfügigsten Onlinegeschäften mit Kreditkartenzahlung.
- die Anwendbarkeit der DSGVO verneint wird, wenn ein/e KonsumentIn einer statistischen Gruppe mit bestimmten Merkmalen zugeordnet wird

und die Attribute der Gruppe nicht direkt dieser Person zugeordnet werden. Auch die statistische Zuweisung in eine bestimmte Verhaltensgruppe kann KonsumentInnen erheblich benachteiligen.

Probleme aus Sicht der ArbeitnehmerInnen: Aufgrund vieler Beratungen wissen wir, dass

- die Arbeit mit digitalen Werkzeugen und Medien vielfach zum vorherrschenden Merkmal der heutigen Erwerbstätigkeit geworden ist: umfangreiche Nutzung moderner Informations- und Kommunikationstechnologien (zB Laptop, Smartphone …) und AnwenderInnensoftware, computerisierte, vernetzte Maschinen (zB Fertigungsroboter) und Arbeitsmittel, Bewerbungsdatenbanken, Vermittlung von Dienstleistungen über Online-Plattformen (zB Crowdworking), globale Vernetzung und Übermitteln von Beschäftigtendaten in Länder außerhalb der EU mit oftmals geringem Datenschutzniveau, etc.

- die wirtschaftlichen Chancen dieser Digitalisierung zu nutzen sind, aber – aufgrund der Tatsache, dass die technischen Möglichkeiten der Überwachung am Arbeitsplatz und der Verwendung von ArbeitnehmerInnendaten immer vielfältiger werden – auch die Rechte der Beschäftigten zu schützen sind.

- im Zusammenhang mit der voranschreitenden Digitalisierung der Arbeitswelt diese Aufgabe immer wichtiger wird und die entsprechenden Herausforderungen enorm sind: Die IT-Systeme werden immer vielfältiger und komplexer, die Menge der dabei generierten und verwendbaren Beschäftigtendaten nimmt exponentiell zu und auch die technischen Verknüpfungs- und Analyse-Möglichkeiten dieser Daten werden immer ausgereifter und aussagekräftiger, bis hin zum Erstellen von Verhaltensvorhersagen von ArbeitnehmerInnen (Profiling) und dem Einsetzen automatisierter Entscheidungsfindungen im Bereich der Personalverwaltung.

- für den Schutz von ArbeitnehmerInnen vor Datenverarbeitungen, die ihre Interessen gefährden, vor allem Mitbestimmungsrechte entscheidend sind: Das können Zustimmungs- bzw Vetorechte der einzelnen Beschäftigten gegenüber Datenverarbeitungen sein, aber vor allem auch – angesichts der Verhandlungsunterlegenheit der einzelnen Beschäftigten gegenüber dem Arbeitgeber (siehe dazu auch die nächsten Punkte) – Zustimmungs- bzw Vetorechte von betrieblichen Interessenvertretungen.

- die Einwilligung als Rechtsgrundlage für die Verwendung personenbezogener Daten nicht zwischen gleichberechtigten VertragspartnerInnen stattfindet, sondern vielmehr ArbeitnehmerInnen im Rahmen der Unterfertigung des Arbeitsvertrags auch die Einwilligung zur Datenverarbeitung vorgelegt wird, womit die Freiwilligkeit sowie das Koppelungsverbot, wie die DSGVO sie verlangt, unterlaufen werden.

- ArbeitnehmerInnen im aufrechten Arbeitsverhältnis ihre Rechte – aufgrund des gegebenen Machtungleichgewichts – so gut wie nie einfordern, also die Möglichkeit, eine Beschwerde bei der Datenschutzbehörde bzw eine Klage bei Gericht einzubringen, nicht in Anspruch nehmen. Um dem entgegenzuwirken und die Rechtsdurchsetzung zu stärken, wäre ein explizites Verbandsklagerecht von großer Bedeutung.

- die Beauskunftung von Datenverarbeitungen oft nur mangelhaft geschieht sowie in einer nicht leicht verständlichen Sprache, womit die Informationsrechte der betroffenen ArbeitnehmerInnen in der Praxis nicht im Sinne der DSGVO ausgeführt werden.

- die Befragung der betroffenen ArbeitnehmerInnen und ihrer Interessenvertretungen im Rahmen der Datenschutz-Folgenabschätzung nur sehr ungenügend durchgeführt wird bzw in den meisten aus der Beratungspraxis bekannten Fällen gänzlich unterbleibt. Somit wird dieses vorab durchzuführende und daher wesentliche – und als einziges in der DSGVO verbliebene – Recht der betroffenen ArbeitnehmerInnen und ihrer betrieblichen Interessensvertretung, zu den Auswirkungen auf ihre Freiheiten und Grundrechte befragt zu werden, meist ignoriert.

3. Exzellente Verbesserungsvorschläge liegen bereits am Tisch

Hierzu verweisen wir etwa auf das Gutachten im Auftrag des Bundesverbands der Verbraucherzentralen (Evaluation der DSGVO aus Verbrauchersicht, Projektgruppe verfassungsverträgliche Technikgestaltung, Univ.-Prof. Dr. A. Roßnagel, 26.11.2019; https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf).

Darüber hinaus schlagen wir vor:

- Die **Rechtsgrundlage „Vertragserfüllung"** (Art 6 Abs 1 lit b) ist zu präziseren. Nur objektiv unbedingt notwendige Daten dürfen auf dieser Basis verarbeitet werden. In der Praxis benutzte vage Gründe, wie „die Verbesserung unserer Dienste" oder „die Optimierung der Kundenerlebnisse" dürfen nicht mehr dazu zählen.

- Zu den Bedingungen für die **Einwilligung im Arbeitsverhältnis** (Art 7): Aufgrund des im Arbeitsverhältnis herrschenden Machtungleichgewichts zwischen Arbeitgeber und ArbeitnehmerInnen trauen sich letztere oft nicht, die Zustimmung zu Datenverarbeitungen zu verweigern. Dass es in Anbetracht aller Umstände in solchen Fällen unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde und diese daher keine gültige Rechtsgrundlage für vorgenommene Datenverarbeitungen darstellen kann, ist im Erwägungsgrund 43 explizit anzuführen.

- **Alle konkreten EmpfängerInnen** von Daten müssen in den Vorabinformationen ausgewiesen werden (Art 13 und 14 Abs 1 lit e). In begründeten Fällen (zB häufige Änderungen) reicht es, wenn die einzelnen EmpfängerInnen erst im Rahmen eines Auskunftsersuchens bekanntgegeben werden (Art 15 Abs 1 lit c). Nur so können KonsumentInnen auch diesen gegenüber ihre Rechte wahrnehmen. Derzeit sucht sich der Verantwortliche in der Praxis selbst aus, ob er EmpfängerInnen oder nur nicht näher bestimmte „Empfängerkreise" beauskunftet.

- AuskunftswerberInnen sollen die **konkreten Datenquellen** (Art 15 Abs1 lit g) erfahren. Derzeit sind nur „verfügbare" Angaben über die Datenherkunft zu beauskunften. Weiters sind derzeit die Verantwortlichen weder zur Speicherung der Datenherkunft nur zum Zweck der Beauskunftung noch zu ihrer nachträglichen Erhebung verpflichtet. Mit einer Dokumentationspflicht der Datenherkunft ginge künftig die Schutzbehauptung ins Leere, die Datenquelle sei nicht „verfügbar".

- Der **Bestimmtheitsgrad reicht für eine unmittelbar anwendbare Verordnung** nicht. Entweder spezifizieren EU-Rechtsakte sektorspezifische Fragen und Interessenskonflikte oder die Mitgliedstaaten erhalten auch in Bezug auf den VerbraucherInnendatenschutz (ähnlich den Öffnungsklauseln für Wissenschaft und den Beschäftigtenkontext) nationale Präzisierungschancen. Das Datenschutzbedürfnis der VerbraucherInnen ist im Zuge der Technikentwicklung (Internet der Dinge, Profiling usw) enorm gewachsen. Die Verordnung regelt den Datenschutz sehr allgemein und abstrakt. Sie geht auf die konkreten Gefährdungslagen datenschutzsensibler Bereiche der Privatwirtschaft nicht näher ein. Für VerbraucherInnen und ihr Bedürfnis nach Rechtssicherheit ist unzumutbar, tausende Detailfragen im Wege langwieriger Aufsichts- oder Gerichtsverfahren klären zu lassen.

- Die Regeln über **automatisierte Entscheidungen und Profiling** (Art 22) schützen Betroffene nur im Falle vollautomatisierter Bewertungen, die Rechtsfolgen haben bzw erheblich beeinträchtigen können. Die beiden Voraussetzungen sind zu streichen. KonsumentInnen und ArbeitnehmerInnen sind auch vor „bloßer" Intransparenz und Manipulation (etwa in Social Media oder in plattformbasierter Arbeit) durch Vorabinfos und Auskunft über die Logik und Tragweite zu schützen. Wann automatisierte Verarbeitungen und Profiling für die Vertragserfüllung überhaupt nötig sein sollen, ist restriktiv zu präzisieren. Die Behauptung, Entscheidungsprozesse seien nur teilautomatisiert und böten am Ende nur die Grundlage für eine menschliche Entscheidung, darf den Schutz der Betroffenen ebenfalls nicht schmälern: auch Entscheidungen „bloß" vorbereitende, „halbautomatisierte" Bewertungen sind einzubeziehen.

- Profiling, Scoring und Verhaltensprognosen mit Hilfe von **Algorithmen, maschinellem Lernen und künstlicher Intelligenz** (Art 22) können VerbraucherInnen- und ArbeitnehmerInneninteressen gefährden. VerbraucherInnen- und ArbeitnehmerInnenverhalten, persönliche Eigenschaften uvm sollen unter deutlich strikteren Kautelen analysiert, klassifiziert oder prognostiziert werden als derzeit. Der im Weißbuch zu künstlicher Intelligenz COM (2020) 65 vorgeschlagene Zwei-Stufen-Test kommt diesem Anliegen nur teilweise entgegen. Demnach würden nur Anwendungen strengeren Vorgaben

unterworfen sein, wenn Anwendungsbereich und die konkrete Anwendung besonders risikogeneigt sind. Alle anderen Datenverarbeitungen unterlägen bloßer freiwilliger Selbstkontrolle. Abgestufte Pflichten für alle – auch niedrigere – Risikoklassen sind nötig. Die Bewertungsanlässe und Datenarten sind restriktiv zu regeln. Derzeit bleibt offen, wann eine automatisierte Entscheidungsfindung überhaupt für einen Vertrag „erforderlich" ist (es fehlen zB Bagatellgrenzen), welche Datenarten maximal verarbeitet werden dürfen (zB kein Mix aus persönlichen Daten und rein statistischen Zuschreibungen) und welche qualitativen Anforderungen man an die Aussagekraft von Prognosewerkzeugen stellt, damit Betroffene nicht willkürlichen und diskriminierenden Bewertungen ausgesetzt sind.

- **Automatisierte Entscheidungen** im Einzelfall und **Profiling im Arbeitsverhältnis** (Art 22) sind nicht erforderlich und dürfen daher nicht zulässig sein. Nach unseren Erfahrungen sind automatisierte Entscheidungsfindungen sowie Profiling weder zur Erfüllung des Arbeitsvertrags „erforderlich" (Art 22 Abs 2 Buchst a), noch kann die Freiwilligkeit einer Einwilligung durch die ArbeitnehmerInnen aufgrund des im Arbeitsverhältnis vorherrschenden Machtungleichgewichts angenommen werden (Art 22 Abs 2 Buchst c). ArbeitnehmerInnen fürchten um die Wertschätzung für ihre menschliche Arbeit: Werden die ArbeitnehmerInnen noch als individuelle Personen wahrgenommen oder wird menschliche Arbeit zukünftig immer mehr wie automatisierte und (leicht) automatisierbare Prozesse definiert und bewertet? Daraus entsteht die Gefahr, dass man mit dieser Übersetzung aller Arbeitsbereiche in eine „Datenwelt", der vermehrt und technikgläubig oberste Geltung und primäre Berücksichtigung zugesprochen wird, auch im Arbeitsprozess zu einem absolut technikzentrierten und damit inhumanen Menschenbild gelangt. Die Arbeitsleistung der ArbeitnehmerInnen wird zunehmend in Zahlen ausgedrückt, gemessen, verglichen, analysiert und es werden daraus folgend automatisiert Entscheidungen und Vorhersagen getroffen. Der Mensch am Arbeitsplatz wird zu einem bloßen messbaren Produktions- und Kostenfaktor herabgewürdigt; der immaterielle Wert der Arbeit und die Würde der Arbeitenden bleiben dabei auf der Strecke. Die Wahrung der Menschenwürde und der Persönlichkeitsrechte sind auch bei der Erbringung der Arbeitsleistung sicherzustellen. Die DSGVO muss ein klares Bekenntnis dazu abgeben und automatisierte Entscheidungen im Einzelfall und Profiling im Arbeitsverhältnis daher untersagen. Dies hat auch für menschliche Entscheidungen „bloß" vorbereitende, „halbautomatisierte" Bewertungen zu gelten.

- Die Auflagen für **Direktwerbung** (Art 7 Abs 3; EG 47) müssen auf KonsumentInnenwünsche Bedacht nehmen. KonsumentInnen wollen eigentlich immer um ihre Zustimmung zu Marketingaktivitäten gefragt werden. Statt einer unsachlichen Privilegierung der Direktwerbung durch bloße Widerrufsrechte sollen VerbraucherInnen ausdrückliche Zustimmungsrechte zur Marketingnutzung ihrer Daten erhalten. Art 21 Abs 2 iVm EG 47 (Widerspruchsrecht bei Direktwerbung; „Direktwerbung kann ein berechtigtes Interesse des Auftraggebers sein") ist dahingehend einzuschränken, dass es sich ausschließlich um Werbung von AnbieterInnen, bei dem die Konsument Innen bereits KundInnen sind, für eigene ähnliche Produkte handeln darf.

- Der **Erlaubnistatbestand „berechtigte Verarbeitungsinteressen"** (Art 6 Abs 1 B f) soll kein Freibrief sein. DatennutzerInnen müssen das Überwiegen ihres Interesses gegenüber den Geheimhaltungsinteressen der VerbraucherInnen belegen. Die Vorgabe, dass bei „berechtigtem Interesse" des Datennutzers oder eines Dritten die Verarbeitung rechtmäßig ist, sofern nicht die Geheimhaltungsinteressen der KonsumentInnen „überwiegen", entspricht faktisch einer Beweislastumkehr zulasten der KonsumentInnen. Unternehmen stützen sich in der Praxis exzessiv auf diese Rechtsbasis, um das Einholen von Zustimmungen zu vermeiden. Um die Lage zu verbessern, sollten im KonsumentInnenalltag gängige Verarbeitungspraktiken aufgezählt werden, bei denen stets die Zustimmung einzuholen ist. Wie das Überwiegen des Interesses nachvollziehbar begründet werden muss, ist zu regeln.

  Derzeit dominieren in der Praxis vage Begriffe wie „Verbesserung unserer Dienste und des Kundenerlebnisses, Betrugsprävention, Direktmarketing, Missbrauchskontrolle und die Datenweitergabe zwischen verbundenen Konzernunternehmen". Die Aufnahme eines Katalogs an möglichst konkreten Erlaubnistatbeständen, die die Geheimhaltungsinteressen der Betroffenen nicht oder nur unwesentlich tangieren, sollte dabei helfen. Auch im Arbeitsverhältnis erweist sich der Erlaubnistatbestand **„berechtigte Verarbeitungsinteressen"** (Art 6 Abs 1 Buchst f) aus vorgenannten Gründen (faktische Beweislastumkehr) und dem hinzukommenden Machtungleichgewicht (ArbeitnehmerInnen trauen sich während des aufrechten

Arbeitsverhältnisses nicht zu widersprechen) als problematisch. Schutzmaßnahmen zugunsten der ArbeitnehmerInnen sind dringend vorzusehen.

- Die **Zweckbindung** (Art 5 Abs 1 lit b) darf nicht mehr durch vage Grundsätze für die Weiterverarbeitung von Daten für andere Zwecke (Art 6 Abs 4) unterlaufen werden. Daten dürfen nur für (im Erhebungszeitpunkt) eindeutig festgelegte Zwecke verwendet werden. Eine automatische spätere Weiterverwendung der Daten für andere Aufgaben sollte untersagt sein. Sollen Daten für andere als die ursprünglichen Zwecke weiterverwendet werden, braucht es immer eine neue Zustimmung der KonsumentInnen. Der Zweckbindung ist wieder Geltung zu verschaffen durch Streichung der Weiterverwendung für andere „vereinbare" Zwecke. Ein Vereinbarkeitstest anhand von unbestimmten Kriterien wie „Zusammenhänge", Datenarten, „vernünftige" Erwartungen, mögliche Folgen oder Garantien hat sich nicht bewährt. KonsumentInnen haben maximale Rechtsunsicherheit und müssten jeden Einzelfall zwecks Vornahme einer rechtssicheren Abwägung einklagen.

- Dem Grundsatz der **Datensparsamkeit** (Art 5 Abs 1 lit c) ist Rechnung zu tragen. Andernfalls haben wir es mit totem Recht zu tun. „Datenreichtum" ist die Gegenwartsdevise. Datenwirtschaft sucht nach immer mehr Daten aus unterschiedlichsten Quellen und Verarbeitungskontexten, die miteinander korreliert werden und dadurch Hinweise auf Zusammenhänge liefern. Die Anforderungen an die Pflicht zur Datenminimierung sind zu konkretisieren. Klarzustellen ist, dass der Grundsatz nicht dadurch umgangen werden kann, dass Daten mit Personenbezug in nicht erforderlichem, maximalen Umfang erhoben werden, nur um sie anschließend pseudonymisiert oder anonymisiert für verschiedenste Zwecke zu nutzen. Zu viele personenbezogene Daten werden nämlich rechtsgrundlos erhoben, nur um sie anschließend verschlüsselt oder anonymisiert für kommerzielle bzw wissenschaftliche Zwecke weiternutzen zu können.

- Die **Öffnungsklausel Wissenschaft, Forschung, Statistik** (Art 89) ist zu weitreichend. Es braucht sektorspezifischen Datenschutz, damit Trends wie Big Data-Anwendungen, Entscheidungen durch Algorithmen und künstliche Intelligenz nicht zulasten der Datenschutzinteressen der KonsumentInnen gehen. Was eine wissenschaftliche Einrichtung überhaupt ist, ist nicht determiniert (auch Internetriesen betreiben bspw Marktforschung). Es fehlt eine klare Grenze zu kommerziellen Aktivitäten. Damit die Freizeichnung von der DSGVO für Zwecke von Wissenschaft und Forschung in vertretbarem Rahmen bleibt, muss definiert sein, wer die privilegierten Institutionen sind. Dabei muss bescheinigt werden, dass der Forschungsgegenstand im öffentlichen Interesse liegt.

  Verantwortliche dürfen nicht pauschal von der Beachtung der Betroffenenrechte entbunden werden. Die Zustimmung der Betroffenen ist stets einzuholen. Einzelzustimmungen sollen nur durch eine Genehmigung der Datenschutzbestimmung (DSB) ersetzt werden können und das auch nur, wenn ein herausragendes öffentliches Interesse am Forschungsgegenstand besteht und Zustimmungen schwer eingeholt werden können. In diesen Fällen ist Betroffenen ein Widerspruchsrecht einzuräumen.

- Das in der DSGVO angelegte **Koppelungsverbot** (Art 7 Abs 4, EG 43- Einwilligung ohne Zwang, Wahlfreiheit ohne Nachteil, Vertragserfüllung unabhängig von Datenverarbeitung) ist außer Streit zu stellen. Dies ist auch in Hinblick auf die Verhandlungen zur e-Privacy Verordnung nötig. So enthält etwa das Ratsdokument vom 8. November 2019 Festlegungen, die dem Koppelungsverbot widersprechen ("Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end-user of a genuine choice…")

- Art und Umfang der **Protokollierungspflichten** (Art 32) sind näher zu regeln (nicht zuletzt, um Datenquellen und algorithmische Entscheidungen nachvollziehbar zu machen).

- Die Grundsätze von **privacy by design und by default** sind zu präzisieren. Die Anforderungen sind zu unbestimmt, um daraus rechtssicher die genauen Pflichten des Verantwortlichen abzuleiten („Unter Berücksichtigung des Stands der Technik, Implementierungskosten, Art, Umfang, Umstände, Risiken…").

- Pflichtstandards für eine verlässliche **Anonymisierung** (Art 4 Abs 1, Art 32) sind einzuführen. Wann Daten als nicht rückführbar anonymisiert gelten, ist derzeit nicht geregelt. Viele ExpertInnen gehen davon aus, dass konkrete Personen auch aus anonymisierten Datensätzen durch Einsatz fortschrittlicher Techniken individuell bestimmbar sind. Es ist zu definieren, wann man (überhaupt noch) von Daten ohne Personenbezug reden kann.

- Missbrauchsrisiken realisieren sich oft aufgrund zu langer **Speicherdauer**. KonsumentInnen und ArbeitnehmerInnen sowie deren Interessenvertretungen können präzisere und kürzere Aufbewahrungsfristen schwer durchsetzen, da sie die Angemessenheit der Fristangaben selten beurteilen können. Die DSGVO sollte den Datenschutzausschuss beauftragen, die maximale Aufbewahrungsfristen anhand von Leitlinien für die gängigsten Verarbeitungen zu präzisieren.

- Der **Vorrang der DSGVO** ist abzusichern. Klarzustellen ist, dass das Schutzniveau der DSGVO durch sektorale Rechtsakte, die Erlaubnistatbestände für die Datennutzung enthalten, nicht unterschritten werden darf. Andernfalls besteht das Risiko, dass zur Förderung der Datenökonomie Vorschriften der DSGVO abbedungen und Datenverarbeitungen gestattet werden, die nicht im Einklang mit ihr stehen.

4. Bei der Unterstützung von KonsumentInnen und ArbeitnehmerInnen registrierte Vollzugsdefizite

- Die Ausstattung der Datenschutzbehörden entspricht nicht dem Bedarf, um rasch, sorgfältig, technikkundig und investigativ den vielfältigen Aufsichtsaufgaben nachzukommen.

- Selbst bei der zentralen Beschwerdebearbeitung ist der Verbesserungsbedarf augenfällig: Die Verfahren dauern bis zu den rechtskräftigen Entscheidungen zu lange.

- KonsumentInnen und ArbeitnehmerInnen erleben es als Rückschritt, dass die Vorabgenehmigungspflichten der Vorläufer-RL 95/46/EG abgeschafft wurden. Die ersatzweisen Vorgaben (reine ex-post-Kontrollen und mehr Eigenverantwortung auf Seiten der Datenverarbeitung) haben sich verglichen mit dem vorsorglichen Schutz der Vorläufer-Richtlinie nicht bewährt. Die Verlagerung von einer ex-ante Prüfpflicht in sensiblen Fällen zu einer nachträglichen Aufarbeitung von Rechtsverletzungen samt Schadenersatzansprüchen eröffnet schwerwiegende Schutzlücken, wenn die nachträgliche Kontrolle nicht reibungslos funktioniert.

- EU-Datenschutz- und VerbraucherInnenverbände haben am Tag des Inkrafttretens der Verordnung Verfahren angestrengt, die durch Zusammenarbeit verschiedener DSB zu erledigen wären. Sie sind auch knapp zwei Jahre danach noch überwiegend offen. Damit fehlen bei Rechtsfragen von zentraler, grenzüberschreitender Bedeutung wegweisende Entscheidungen. Ohne rasche, fundierte Entscheidungspraxis können die interpretationsbedürftigen Normen der DSGVO nicht rechtssicher angewandt werden.

- Die Idee einer europaweit einheitlichen Anwendung der DSGVO ist nur so gut wie ihre Umsetzung in der Praxis. Beispielshaft erwähnt sei eine ungeklärte Kardinalfrage: ob und wann besteht ein Koppelungsverbot, darf also der Dienstzugang für InternetnutzerInnen nicht von der Akzeptanz der Verarbeitung von Daten über das zur Diensterfüllung nötige Maß abhängen. Ob und inwieweit Millionen Nutzungsvorgänge bei großen Internetplattformen unrechtmäßig und welche alternativen Abgeltungsformen zulässig sind, kann noch immer nicht verlässlich beantwortet werden.

- Die Zahl nationaler Entscheidungen, die – soweit bekannt – uneinheitlicher nicht sein können, wächst. Eine EU-weite Plattform zur Einsicht nationaler Urteile und Verwaltungsbescheide fehlt. Übersicht und Vergleichbarkeit von Entscheidungen sind damit enge Grenzen gesetzt.

- Rechtsverstöße werden nicht verfolgt, weil KonsumentInnen schwer verständliche Sachverhalte nicht mühsam zusammentragen, um ihre Rechte zu verfolgen. Sie erwarten sich in den gängigsten Risikobereichen der Datenökonomie (Internetplattformen, Scoring-Dienstleister uÄ) nach dem Fürsorgeprinzip präventive Aufsichtsmaßnahmen durch staatliche Behörden.

- Sie wollen bei Bekanntwerden von Verstößen mit möglichen Schadenersatzfolgen ihre Rechte nicht alleine durchsetzen. Verbandsklagen von KonsumentInnenschutzorganisationen sind allerdings nur in Mitgliedstaaten möglich, die diese optionale Möglichkeit im nationalen Recht umgesetzt haben. Schadenersatzansprüche sind auf diesem kollektiven Weg gar nicht einklagbar.

- Die Arbeiterkammer erfährt in ihren Beratungen immer wieder von – zum Teil auch massiven – Datenschutzverstößen durch die Arbeitgeber. ArbeitnehmerInnen haben Angst um ihren Job oder vor Benachteiligungen, wenn sie

dagegen vorgehen. Die Verbandsklagsbefugnis böte Einrichtungen, die mit der Durchsetzung von Datenschutz-, VerbraucherInnen- bzw ArbeitnehmerInnenrechten befasst sind, die Chance, für Datenschutzinteressen von Betroffenen eintreten zu können, ohne dass eine Person mit dem Einbringen einer formellen behördlichen oder gerichtlichen Beschwerde belastet werden muss. Verbandsklagerechte auch für die überbetrieblichen (gesetzlichen und freiwilligen) Interessenvertretungen sind wichtig, um das bestehende Machtungleichgewicht im Arbeitsverhältnis ohne Risiko für betroffene ArbeitnehmerInnen fair auszubalancieren.

5. Wir schlagen vor:

- **DSB-Vorabkontrollpflicht** bei Anwendungen, die der Folgenabschätzung nach der DSGVO unterliegen. KonsumentInnen und ArbeitnehmerInnen erwarten sich vorbeugenden Schutz. Sie möchten Vorsorge statt hinterher das Nachsehen und bloße Schadenersatzansprüche. Um dem deutlichen ExpertInnenruf nach einer Vorabkontrolle der „Fairness" von Algorithmen zu entsprechen, braucht es künftig ohnehin behördliche Prüfpflichten im Vorfeld risikobehafteter Anwendungen. Was für automatisierte Einzelentscheidungen künftig unbedingt nötig ist, sollte für alle Datenverarbeitungen gelten, die einer Folgenabschätzung bedürfen. So können Grundrechtsverletzungen bereits verhindert werden, bevor sie großen Schaden anrichten.

- **Einführung einer verpflichtenden Verbandsklagsbefugnis (in Art 80 Abs 2)** statt einer reinen Option für die Mitgliedstaaten. Das Rechtsschutzinstrument sollte genutzt werden können, um Schadenersatzansprüche geltend zu machen.

- **Bessere Zusammenarbeit der DSBs** mit dem Ziel, Fälle von erheblicher Tragweite für VerbraucherInnen rasch und fundiert zu entscheiden. Auch die Verfahren der Rechtsmittelinstanzen sind in die Verbesserungsmaßnahmen einzubeziehen.

- **Eine zügige Veröffentlichung** sämtlicher Entscheidungen, die in Zusammenarbeit mehrerer DSBs getroffen werden und über ein EU-Rechtsinformationssystem Zugang auch zu nationalen Entscheidungen.

6. Datenschutz wird künftig noch bedeutsamer, denn

es fehlen Geschäftsmodelle, die die Anonymität von OnlinenutzerInnen wahren. Herkömmliche Geschäftsmodelle, bei denen KonsumentInnen eine Leistung bezahlen, werden durch solche verdrängt, bei denen KonsumentInnen mit ihren Verhaltensdaten selbst zum Produkt werden. Geschäfte, die bislang anonym abgewickelt wurden, gehen durch die Digitalisierung verloren. Frank Schirrmacher, ehemaliger Mitherausgeber der Zeitung FAZ, formulierte dazu treffend: „Verbraucherschutz in der Informationsökonomie wird zu einer politisch hochbedeutsamen Aufgabe. Er muss sich zu einem Instrument der Freiheitssicherung entwickeln. Der Verbraucher im digitalen Zeitalter kauft nicht nur ein Produkt, er wird selbst zum Produkt. Er wird gelesen, wenn er kauft. Er wird gelesen, wenn er sich bewegt. Er wird gelesen, wenn er liest, wenn er bezahlt, sogar wenn er denkt."

Mit dem Internet der Dinge wird das Prinzip der Datensparsamkeit ins Gegenteil verkehrt. Schon eine BAK-Studie aus 2014 (https://www.arbeiterkammer.at/infopool/wien/Digitale_Ueberwachung_im_Alltag.pdf) machte auf diese Folge aufmerksam: E-Book-Reader und vernetzte TV-Geräte senden Daten zum NutzerInnenverhalten 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. Überwachungsrisiken und ungeklärte Rechtsfragen liegen offen am Tisch: Wann weisen die Betriebsdaten vernetzter Geräte keinen Personenbezug mehr auf und wem „gehören" sie eigentlich? Wie werden KonsumentInnen vor unrechtmäßigen Zugriffen geschützt und vor einer Weiterverarbeitung zu anderen Zwecken, die sie nicht befürworten (öffentliche Sicherheit, Wissenschaft). Wie schützt man das Selbstbestimmungsrecht der KonsumentInnen in Bezug darauf, bei Alltagsgeschäften auch ohne Nachteil „offline" sein zu dürfen. So zeigte etwa eine BAK-Studie (https://www.arbeiterkammer.at/infopool/wien/Privatsphaere_in_Online-Spielen.pdf), dass populäre digitale Spiele nur mehr mit Onlineverbindung funktionieren. Selbst dann, wenn KonsumentInnen alleine spielen und eine Internetverbindung funktionell nicht

erforderlich ist. Dies widerspricht dem Grundsatz der Datenminimierung. Ohne entsprechende Verbotsnorm dürften NutzerInnen smarter Geräte künftig noch oft gezwungen werden, dem Abgreifen ihrer Daten relativ machtlos zuzusehen.

Außerordentliches **Gefahrenpotential** für eine Verletzung der Privatsphäre besteht dann, wenn **KonsumentInnen zugleich ArbeitnehmerInnen** bei Unternehmen sind, die ihre personenbezogenen Daten sowohl arbeitsbezogen als auch in die Privatsphäre reichend (aus-) nutzen (zB Angestellte in Spitälern oder bei privaten Versicherungsunternehmen, wenn arbeitsseitig installierte Apps zur „Reduzierung des ökologischen Fußabdrucks" die Privatsphäre tracken, wenn Dienstfahrzeuge privat geortet werden, etc). In all diesen Fällen ergibt sich eine doppelte Betroffenheit, die durch das Machtungleichgewicht im Arbeitsverhältnis verstärkt wird.

Echter sektoraler Datenschutz fehlt: Es gibt zu wenig branchen- und technikspezifischen Datenschutz findet bspw der europäische Verbraucherverband BEUC und legte schon 2017/2018 der EU-Kommission detaillierte Forderungspapiere vor:

- ePrivacy Regulation –improvements needed (https://www.beuc.eu/publications/beuc-x-2019-071_letter_to_deputy_pr_ambassador_-_minna_kivimaki_finland_-_eprivacy_regulation.pdf)

- Protecting European Consumers with Connected and Automated Cars (https://www.beuc.eu/publications/beuc-x-201138_dve_beuc_connected_autonomous_cars.pdf)

- Cybersecurity for connected goods (https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf)

- Securing Consumer Trust in the Internet of Things – Principles and Recommendations (https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf)

- Automated Decision Making and Artificial Intelligence – A Consumer Perspective (https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf).

Ungewisse Zukunft der e-Privacy Verordnung: Der DSGVO kommt nur längerfristige Bedeutung zu, wenn sektorspezifische Rechtsakte ihren Anwendungsbereich nicht aushöhlen und Erlaubnistatbestände zur Datennutzung nicht den Vorrang erhalten. Diese Gefahr sehen wir überdeutlich bei der e-Privacy-Verordnung, die zeitgleich mit der DSGVO in Kraft treten hätte sollen. Sie (und deutlich weniger die DSGVO) wird darüber entscheiden, ob InternetnutzerInnen bestmöglichen Daten- und Privatsphärenschutz genießen. Nach derzeitigem Verhandlungsstand ist zu erwarten, dass gemessen am Schutzniveau der geltenden ePrivacy-RL der künftige Standard - geht es nach dem Rat und der Datenökonomie - beschämend gering ausfällt. Manche Vorhaben stehen in klarem Widerspruch zur DSGVO.

So schlug das Ratsdokument vom 8. November 2019 in Bezug auf „Cookie-Walls" folgendes vor: "Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques." Die DSGVO enthält demgegenüber Normen, die wohl nur sinnvoll als Koppelungsverbot gedeutet werden können:

- Art 7 Abs 4: Bei der Beurteilung der Freiwilligkeit einer Einwilligung ist dem Umstand in größtmöglichen Umfang Rechnung zu tragen, ob u.a. die Erfüllung eines Vertrages von der Einwilligung zur Datenverarbeitung abhängig ist, die für die Vertragserfüllung nicht erforderlich ist.

- EG 42: „Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben haben, wenn sie eine echte oder freie Wahl haben und somit in der Lage sind, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden".

- EG 43: „Die Einwilligung gilt nicht als freiwillig erteilt, wenn die Erfüllung eines Vertrages einschließlich der Erbringung eines Dienstes von der Einwilligung abhängig ist, obwohl für die Vertragserfüllung nicht nötig."

Es besteht die Gefahr, dass der Anwendungsbereich der DSGVO durch sektorale EU-Rechtsakte, die der Datenökonomie den Weg bereiten soll, ausgehöhlt wird. Ziel ist, Wachstum und Innovation zu fördern und weniger den Grundrechtsschutz. Es ist mit Erlaubnistatbeständen im Interesse einer florierenden Datenökonomie zu rechnen, die nicht den KonsumentInnenwünschen (weniger Daten, Zustimmung immer vorausgesetzt) entsprechen.

Widerspruch zwischen Datenminimierung und Datenökonomie nicht aufgelöst: Die bisher beschriebenen Entwicklungen widersprechen dem eingangs zitierten Wunsch der VerbraucherInnen nach einer Reduktion unkontrolliert zirkulierender Datenmengen und einer ausnahmslosen Achtung ihrer Zustimmungsrechte. Datengetriebenes Wirtschaften steht seinem Wesen nach unter permanenten Wachstumszwang. Es setzt voraus, dass DatenlieferantInnen, Datenbroker, DatenanalystInnen, technische DienstleisterInnen bis hin zu den KundInnen auf den Datenmärkten Zugriff auf immer mehr Daten erhalten. Data Business und Data Science bedingen das Vorhandensein von „Big Data" am besten in Form von Massendaten, die aus den unterschiedlichsten Quellen in Echtzeit anfallen. So ruhen auch die Hoffnungen, die dem Internet der Dinge vorauseilen, nicht etwa auf dem Verkauf smarter Geräte. Die Aussicht auf zusätzlichen Datenzugang im persönlichsten Umfeld der KonsumentInnen ist vielversprechender. Mithilfe von Algorithmen- bzw KI-Technologien werden Datenbestände verknüpft und analysiert, um neue Erkenntnisse zu gewinnen und kommerziell zu verwerten.

Prinzipien wie Geheimhaltung, Datensparsamkeit und Zweckbindung erodieren aufgrund von Ausnahmen und Interpretationsspielräumen: Wirtschaft und Forschung fordern folgerichtig: es braucht deutlich mehr Daten zum Trainieren von KI, aber auch um (halb)autonomes Fahren möglichst sicher zu gestalten oder zur Steuerung von städtischer Infrastruktur im Rahmen von „smart Cities". Behörden und Politik stehen dem wachsenden Bedarf an Daten nicht nach: mehr Daten zu erheben bzw darauf Zugriff zu erhalten, wird gleichgesetzt mit der besseren Erfüllung öffentlicher Aufgaben, sei es im Bereich der öffentlichen Sicherheit, Bildung, Gesundheit oder des Verkehrs. Kreditinstitute verloren 2018 entsprechend der Zahlungsdienste-Richtlinie 2 ihr Monopol auf Kontodaten: alternative Zahlungsdienste bekommen (mit Zustimmung der VerbraucherInnen) ebenfalls Zugriff.

Die Wettbewerbspolitik erwägt durch zusätzliche Datenportabilität für KonsumentInnen bzw einem verpflichtenden Zugang für MitbewerberInnen zu den Datenbergen die konzentrierte Marktmacht von Internetkonzernen zu brechen. Die Folge könnte sein, dass mehr Unternehmen Zugang zu den Daten der KonsumentInnen haben und diese die exzessiven Datenverwertungspraktiken der großen Internetkonzerne (Medien, Werbenetzwerke, Sharingplattformen und Handelsportale) auch ergreifen.

„Bezahlen mit Daten" statt mit Geld wurde spätestens mit der Anerkennung in verschiedenen EU-Rechtsakten (zB Digitale Inhalte-RL, Omnibus-RL) legitimiert. Diese vordergründig dem VerbraucherInnenschutz dienende Rechtsentwicklung ist ein Paradigmenwechsel für den Grundrechtsschutz: Der Schutz personenbezogener Daten ist als Recht auf informationelle Selbstbestimmung Teil des in Art. 8 EU-Grundrechte-Charta verankertem Persönlichkeitsrechts. Daten als Zahlungsmittel zu sehen, hat bei einigen RechtsexpertInnen zur Annahme geführt, dass das Grundrecht auch schuldrechtlich veräußert werden kann. Andere sehen damit den Wesenskern des Grundrechts verletzt. Die wahren Kosten des Zahlens mit Daten wird erst viel später sichtbar: wenn Verhalten, Meinungen oder Entscheidungen durch Behavioral Targeting manipuliert werden. Insoweit muss „Bezahlen mit Daten" unter einem doppelten Vorbehalt stehen: Einerseits des Grundrechts, das die/der Einzelne mit seiner Zahlungsbereitschaft nicht völlig aufgeben kann, und andererseits einer gesetzlichen Fürsorgepflicht, soweit die/der Einzelne die Konsequenzen der Verarbeitungen und Empfänger seiner Daten nicht abschätzen kann.

Die jüngsten Entscheidungen des EUGH haben zwar das Selbstbestimmungsrecht der VerbraucherInnen formal gestärkt („Planet 49" c-673/17, „Fashion-ID" c-40/17, „Facebook Fanpage" c-210/16 etc). Diese Entscheidungen haben aber nicht spürbar dazu beigetragen, dass VerbraucherInnen über Art und Umfang der Verarbeitungen im Internet nun wirklich besser Bescheid wissen, sie öfter nach ihrer Zustimmung gefragt oder weniger Daten als zuvor verarbeitet werden. Kurz: Im VerbraucherInnenalltag hat sich die DSGVO nur unwesentlich ausgewirkt.

Kontaktieren Sie uns!

In Wien:

Daniela Zimmer
T +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

Martina Chlestil
T +43 (0) 1 501 651 2693
martina.chlestil@akwien.at

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

www.arbeiterkammer.at

In Brüssel:

Peter Hilpold
T +32 (0) 2 230 62 54
peter.hilpold@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 ArbeitnehmerInnen und KonsumentInnen 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.