AK EUROPA

Positionspapier
Juni 2020
EU Allgemein

# Eine europäische Datenstrategie

# Die Position der AK

Die Europäische Kommission hat am 20.02.2020 die künftige europäische Datenstrategie vorgestellt und eine Konsultation eröffnet, an welcher sich die AK gerne beteiligt und neben der Beantwortung des Fragebogens die im Folgenden dargestellten Grundsatzüberlegungen einbringen möchte.

Das Ziel der europäischen Datenstrategie besteht darin, einen einheitlichen europäischen Datenraum zu schaffen und die Sicherheit von allen Daten zu gewährleisten. Mit dieser Strategie soll sichergestellt werden, dass die Bürgerinnen und Bürger im Mittelpunkt der datengetriebenen Wirtschaft stehen, europäische Unternehmen und Behörden die von ihnen erzeugten Daten gewinnbringend nutzen können und einen besseren Zugang zu den von anderen erzeugten Daten haben.

Grundsätzlich begrüßt die AK das Vorhaben einer gemeinsamen europäischen Datenstrategie, weist aber darauf hin, dass noch zahlreiche Überlegungen hinsichtlich umfassenden Datenschutzes, ausgewogener Chancen für VerbraucherInnen und NutzerInnen von Daten sowie fairer Wettbewerbschancen auch für kleine Unternehmen und einer stärkeren Regulierung der großen „Datensammler" in die Strategie einfließen müssen. Als Interessenvertretung aller in Österreich unselbständig Beschäftigten legen wir auch ganz besonderes Augenmerk auf die Auswirkungen der Sammlung und Verarbeitung von Daten über ArbeitnehmerInnen.

## 1. Umfassender Schutz für VerbraucherInnen in einer datenbasierten Wirtschaft

### 1.1. Zusammenfassung unserer Anliegen:

Mit einem Rechtsrahmen „Governance gemeinsamer europäischer Datenräume" soll geklärt werden, welche Daten in welchen Situationen für neue innovative Dienste – unter Einhaltung des Datenschutzes - genutzt werden können. Die AK fordert in diesem Zusammenhang:

- Anonymisierung: eine rechtliche Definition, wann Daten als ausreichend anonymisiert bezeichnet werden dürfen.

- Selbstbestimmungsrechte: Eine Klarstellung, dass auf Basis einer transparenten Aufklärung über Nutzungsvorhaben bei den Betroffenen ausnahmslos Einwilligungen für die Weiternutzung ihrer (anfänglich oder weiterhin personenbezogenen) Daten für kommerzielle bzw Wissenschafts- und Forschungszwecke einzuholen sind. Bloße Widerspruchsrechte sind nur für Anwendungen denkbar, bei denen die Datenschutzbehörde im Rahmen einer Vorabprüfung ein wichtiges öffentliches Interesse und Datenschutzkonformität festgestellt hat. Die Öffnungsklausel in Art 89 Datenschutz-Grundverordnung (DSGVO) für Ausnahmen zugunsten von Wissenschaft oder Statistik ist dahingehend einzuschränken, dass Betroffene sich auf alle Betroffenenrechte nach Art 12 ff DSGVO berufen können müssen. Sensible Daten dürfen ohne ausdrückliche Einwilligung der betroffenen Person für derartige Datenpools nicht herangezogen werden.

- „Datenaltruismus": Die seitens der Kommission angedachten „Datenspenden" setzen von den Datenschutzbehörden vorab geprüfte „Spenderinformationen und -verträge" voraus, damit sich diese über die Tragweite ihrer Entscheidung im Klaren und nicht nur auf spätere

Beschwerden und Schadenersatzansprüche verwiesen sind.

Mit einem „**Rechtsakt über Daten**“ sollen „Nutzungsrechte an gemeinsam erzeugten IoT-Daten (Internet der Dinge, Anm.) und Regeln für die verantwortungsvolle Nutzung von Daten (zB die rechtliche Haftung) präzisiert werden“. Die AK fordert in diesem Zusammenhang folgende **flankierende Regeln zum Schutz der KonsumentInnen, die IoT-Geräte nutzen**:

- Die Eigentümer smarter Geräte können völlig autonom über das gekaufte Produkt verfügen;
- Sie haben ein Verfügungsrecht an allen Softwarekomponenten und ein uneingeschränktes Selbstbestimmungsrecht über alle Daten, die das Produkt erzeugt;
- Sie können ohne Zwang darüber entscheiden, ob und wem sie Daten zugänglich machen;
- Sie dürfen Reparatur- und Servicebetriebe frei wählen, woraus sich auch der Anspruch ableitet, dass der gewählte Betrieb Zugang zu den erforderlichen Daten erhält;
- Sie dürfen nicht gezwungen sein, Koppelungsverträge zu akzeptieren (Warenkauf plus Wartungs- und Serviceverträge oder Versicherungen, die ein Tracking der Produktbenutzung beinhalten);
- Sie müssen darauf vertrauen können, dass sich Hersteller bzw Verkäufer nicht auf Haftungs- und Gewährleistungsausschlüsse berufen, wenn sie sich ihre Servicebetriebe frei aussuchen oder nicht alle anfallenden Daten zugänglich machen.
- Sie müssen die Grundfunktionen aller smarten Geräte auch offline nutzen können;
- Sie müssen sich auf hohe Cybersecurity-Standards verlassen können, deren Einhaltung behördlich geprüft wird.
- Sie müssen durch eine Solidarhaftung von Geräteherstellern, Softwarelieferanten, Serviceanbietern und Verkäufern vor haftungsrechtlichen Zuordnungsproblemen geschützt sein.

Unter dem Titel „**Kompetenzen**“ wird angekündigt, dass „Einzelpersonen bei der Durchsetzung ihrer Rechte in Bezug auf die Nutzung der von ihnen erzeugten Daten unterstützt werden“. Mithilfe neuer Tools sollen sie darüber entscheiden können, was mit ihren Daten geschieht („persönliche Datenräume“) und Kontrolle über ihre Daten ausüben. Die AK gibt in diesem Zusammenhang zu Bedenken:

- **fraglicher Mehrwert**: BürgerInnen bzw KonsumentInnen sind in ihrem (digitalen) Alltag stark gefordert. Datenverwaltungsaufgaben überantwortet zu bekommen, stellt für viele eine zeitliche und informationelle Zusatzbelastung dar. Privacy by Design und Default (also etwa Auswahlmöglichkeiten durch Datenschutz-Einstellungen) und Datenportabilität sind in der DSGVO längst verankert und müssen bei allen Diensten umgesetzt sein. Neue Tools können sich somit nur auf das sehr schmale Feld von nicht personenbezogenen Daten beziehen.
- **Datenmittler**: Seriosität, Kompetenz und Unabhängigkeit von Datentreuhändern müssten behördlich geprüft werden, sonst drohen auf dieser Ebene neue Risiken des Datenmissbrauchs. KonsumentInnen haben wenig Bedarf, ihre Daten von einem Dritten verwalten zu lassen, solange dieser nicht Gewähr dafür leistet, dass diese datenschutzkonform verwendet werden und dies notfalls auch durchsetzt. Diese Marktwächterrolle haben aber in erster Linie Datenschutzbehörden und Verbraucherschutzvereine zu erfüllen.

## 1.2. Zum Hintergrund unserer Anliegen:

### 1.2.1 Bezüglich personenbezogener Daten

**Förderung datengetriebener Wirtschaft setzt mehr Verbraucher- bzw Datenschutz voraus**: Politik, Wirtschaft und Forschung stellen gerade die Weichen für eine datengesteuerte Wirtschaft (siehe neben der Mitteilung zur EU-Datenstrategie COM (2020) 66 ua auch das Weißbuch zu künstlicher Intelligenz COM (2020) 65, die Mitteilungen COM (2020) 66 über eine europäische Datenwirtschaft und COM (2018) 283 über den Weg zur automatisierten Mobilität). Auszug aus der aktuellen KOM-Mitteilung: „Die von Daten vorangetriebene Innovation wird den BürgerInnen enorme Vorteile bringen (personalisierte Medizin, neue Mobilität, Beitrag zum Grünen Deal).

**AK- Anliegen:** Den Schattenseiten der Entwicklung ist in der Debatte mehr Raum zu geben. Unter Druck geratene Selbstbestimmungsrechte über Daten, Datensicherheit, Freiheit von Überwachungszwängen, Benachteiligung von „Offlinern“ und Personen, die nicht jeden Digitalisierungstrend mitmachen wollen, und jenen, die durch algorithmische Entscheidungen bspw diskriminiert werden, verdienen gleichermaßen Beachtung.

**Personenbezug oder doch nicht?** In den zuvor genannten Mitteilungen werden Daten mit und ohne Personenbezug angesprochen und solche, bei denen der Personenbezug mehr oder weniger verlässlich entfernt wurde. Säuberlich getrennt wird selten. Eine Bewertung der Kommissionsvorhaben setzt Klarheit voraus, von welcher Datenkategorie gerade die Rede ist. Sehr zum Nachteil der KonsumentInnen gibt es keine eindeutige rechtliche Grenze zwischen den einzelnen Datenkategorien.
Auch bezüglich (angeblich) anonymisierten Daten behaupten ExpertInnen, dass durch fortschreitendes maschinelles Lernen so gut wie jede Anonymisierung auf ein Individuum zurückgeführt werden kann: KonsumentInnen werden re-identifizierbar.

**AK-Anliegen**: Wann ein Personenbezug noch vorliegt und wann Daten technisch wie organisatorisch als irreversibel anonymisiert gelten, ist derzeit rechtlich nicht beantwortet. Hier besteht dringender Handlungsbedarf.

**Konsumentenvertrauen**: Die AK teilt die Auffassung der Kommission, dass KonsumentInnen „datengetriebenen Innovationen" nur dann vertrauen, wenn bei jeder Weitergabe personenbezogener Daten Datenschutznormen eingehalten werden. Die DSGVO erfüllt Konsumentenbedürfnisse (noch) nicht: KonsumentInnen entscheiden aktuell nicht wirklich selbstbestimmt über ihre Daten. Dem Anliegen von zwei Drittel der in einer Eurobarometer-Umfrage Befragten wird in der Praxis nicht entsprochen: diese gaben nämlich an, dass sie vor jeder Datennutzung nach ihrer Zustimmung gefragt werden wollen.

**AK-Anliegen**: Es sind zusätzliche Anstrengungen nötig, sollen die Selbstbestimmungsrechte der KonsumentInnen in einer Datenökonomie, die nach immer mehr Daten für immer mehr Zwecke verlangt, maßgeblich verbessert werden. Einer datengetriebenen Wirtschaft wird nur dann vertraut, wenn Schwachstellen in der DSGVO nachgebessert, Datensicherheitsstandards verbindlich geregelt und eklatante Vollzugsdefizite verringert werden.

„**Making more data available**" lautet die Devise. Die vorgestellten Maßnahmen sollen das Angebot und die Nachfrage nach Daten steigern. „Für eine innovative Weiterverwendung von Daten, darunter auch zur Entwicklung künstlicher Intelligenz, stehen gegenwärtig nicht genügend Daten zur Verfügung. Die bestehenden Probleme lassen sich danach gruppieren, wer Dateninhaber und wer Datennutzer ist, hängen aber auch von der Art der Daten ab (personenbezogene Daten, nicht-personenbezogene Daten oder gemischte Datensätze, die beides enthalten)". Der europäische Weg sei es, „den Austausch und die breite Nutzung von Daten zu kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethikstandards zu wahren". „In einer Gesellschaft, in der jeder Einzelne immer größere Datenmengen erzeugt", müsse „die Art und Weise, wie Daten gesammelt und verwendet werden, zuallererst den Interessen des Einzelnen entsprechen – ganz im Einklang mit den europäischen Werten, Grundrechten und Vorschriften".

**AK-Anliegen**: Ein Mangel an Daten ist kein „Problem", sondern Teil der Lösung: nach der DSGVO dürfen Daten nur für konkrete Zwecke entsprechend dem Prinzip der Zweckbindung und Datensparsamkeit erhoben werden. Auch der Aussage, Personen würden immer mehr Daten erzeugen, ist entgegenzuhalten, dass kein Konsument von sich aus willentlich und wissentlich große Datenmengen erzeugt.
Vielmehr sind es die Anbieter von elektronischen Diensten, die Onlinewerbewirtschaft usw, deren Datenerhebung und Geschäftsmodelle im eklatanten Widerspruch zu strafbewehrten Geboten wie Datensparsamkeit, Zweckbindung und Privacy by Design und Default stehen.

**Widerspruch zwischen Datenökonomie und Geboten wie Datensparsamkeit ungelöst**: In Aussicht gestellt wird in den Mitteilungen ein in der Realität oft nicht einlösbares „sowohl als auch" von Datenökonomie und Grundrechten. Gebraucht wird ein ehrliches Bekenntnis, dass manchmal nur eine Option des „entweder oder" besteht: Auswertung von großen Datenpools für unbestimmte Zwecke oder ein hohes Datenschutzniveau. Der Entwicklung zum „Datenreichtum" einer Datenökonomie steht bei personenbezogenen Daten der bereits erwähnte Grundsatz der Datensparsamkeit entgegen. Auch anonymisierte Daten basieren auf zunächst personenbezogen erhobenen Daten, für die die Zulässigkeitsvoraussetzungen und das Sparsamkeitsgebot der DSGVO gelten. Viele personenbezogene Daten werden rechtswidrig erhoben, ohne erforderlich zu sein und eine taugliche Rechtsgrundlage zu haben, nur um sie anschließend verschlüsselt für kommerzielle oder auch wissenschaftliche Zwecke weiternutzen zu können. Vor allem der Bedarf von künstlicher Intelligenz nach immer mehr Trainingsdaten widerspricht oft nicht nur dem Gebot der Datensparsamkeit, sondern auch der Zweckbindung und von privacy by design bzw default.

**AK-Anliegen**: Privatsphäre und Datenschutz ist im Fall eines unlösbaren Konfliktes mit Erwerbsfreiheiten der Vorrang einzuräumen. Die Pflicht zur Datenminimierung muss konkretisiert werden. Klarzustellen ist, dass das Gebot nicht dadurch umgangen werden kann, dass Daten

mit Personenbezug rechtlich ungedeckt erhoben und kurzzeitig gespeichert werden, nur um sie pseudonymisiert oder anonymisiert für weitere Zwecke zu nutzen.

KonsumentInnen beklagen, dass

- Datenverantwortliche selten ihre Zustimmung einholen und sich damit rechtfertigen, dass nicht überprüfbare, überwiegende berechtigte Interesse des Unternehmens oder Dritter an der Verarbeitung bestünden.

- ihre Daten nicht physisch gelöscht, sondern nur anonymisiert werden. Ob und wie verlässlich anonymisiert wird, ist ungewiss. Mangels Normen und Nachweisen besteht Unsicherheit, ob ein Rückschluss auf ihre Person wirklich ausgeschlossen ist. Außerdem ärgert es KonsumentInnen, wenn basierend auf ihren Verhaltensdaten statistische Analysen gemacht und verkauft werden.

- ihnen Einblick in algorithmische Entscheidungsprozesse mit der Begründung verwehrt wird, die Entscheidung erfolge „nur" teilweise automatisiert oder die Bewertung sei nicht mit rechtlichen oder „erheblich" beeinträchtigenden Folgen für den Verbraucher verbunden.

- Daten jahrelang gespeichert werden, ohne dass KonsumentInnen die Angemessenheit abschätzen können. Wie lange Daten tatsächlich "erforderlich" sind, ist kaum prüfbar.

- so gut wie nie die genauen Empfänger ihrer Daten beauskunftet werden, sondern nur „Empfängerkreise", weil Unternehmen aus der DSGVO ein Wahlrecht ableiten und so gut wie nie Auskunft über die Herkunft der Daten erteilt wird, weil Unternehmen nur „verfügbare" Informationen beauskunften müssen und diese daher praktisch nie verfügbar sind.

- sie mit der Weitergabe ihrer Daten (zB Standortdaten) für wissenschaftliche oder statistische Zwecke in für den Verwender pseudonymisierter oder anonymisierter Form nicht einverstanden sind. Sie sind verärgert, wenn ihnen nur Widerrufs- statt Zustimmungsrechte eingeräumt oder gar überwiegende berechtigte Interessen entgegengehalten werden.

AK-Anliegen: Eine Vorabkontrollpflicht der Datenschutzbehörden bei Anwendungen, die einer Folgenabschätzung nach der DSGVO unterliegen. Denn KonsumentInnen erwarten sich vorsorglichen Schutz. Sie möchten Vorbeugung statt bloße Schadenersatzansprüche bei Verstößen. Um dem Kommissionsvorschlag nach einer Vorabkontrolle der „Fairness" risikobehafteter Algorithmen (siehe Mitteilung zu künstlicher Intelligenz) zu entsprechen, braucht es künftig ohnehin behördliche ex ante-Prüfungen. So können Grundrechtsverletzungen verhindert werden, bevor sie großen Schaden anrichten.

Außerdem:

- Vorrang für Zustimmungsrechte: die Rechtsgrundlage „berechtigte Interessen" soll nur in rechtlich klar definierten Ausnahmenfällen herangezogen werden,

- Protokollierungs- und Auskunftspflicht über alle konkrete Datenquellen und -empfänger,

- Info- und Auskunftsrechte bei jeder algorithmischen Entscheidung (auch wenn teilweise automatisiert und unabhängig von „erheblichen Beeinträchtigungen" der KonsumentInnen),

- Wahlrecht der Betroffenen zwischen physischer Löschung oder Anonymisierung,

- Leitlinien für die maximale Aufbewahrungsdauer der Daten in gängigen Situationen und für die Umsetzung von privacy by design und default,

- Klarstellung des umstrittenen Koppelungsverbots zwischen Zustimmung zur Datennutzung und dem Zugang zu Diensten,

- voller Umfang der Betroffenenrechte auch bei Nutzung der Öffnungsklausel zugunsten nationaler Vorschriften für Wissenschaft und Forschung,

- keine Weiternutzung von Daten für andere „kompatible" Zwecke ohne Nachweis einer gesonderten Rechtsgrundlage,

- Betroffenenrechte auch bei statistischen Zuschreibungen,

- eine bessere Ausstattung der Datenschutzbehörden, um rasch, sorgfältig, technikkundig und investigativ den vielfältigen Aufsichtsaufgaben nachkommen zu können und

- raschere Verfahren – denn es fehlen bei Rechtsfragen von zentraler, grenzüberschreitender Bedeutung wegweisende Entscheidungen. Ohne diese können die interpretationsbedürftigen Normen der DSGVO nicht rechtssicher angewandt werden.

**Sektorspezifische Rechtsakte**: Sektorspezifische Rechtsakte höhlen die Vorgaben der DSGVO aus. Diese Gefahr sehen wir überdeutlich bei der e-Privacy-Verordnung. Nach derzeitigem Verhandlungsstand ist zu befürchten, dass gemessen an der geltenden e-Privacy-RL das künftige Schutzniveau beschämend gering ausfällt. Noch ein Beispiel: Mehr als 20 elektronische Assistenzsysteme sind nach der EU-VO zur Fahrzeugsicherheit in Autos künftig verpflichtend einzubauen. Darunter ein Unfalldatenspeicher, der sich als „Datenkrake" für Versicherungen, Polizei, Behörden und die Forschung erweisen kann.

**AK-Anliegen**: Erlaubnistatbestände zur weitreichenden Datennutzung in sektorspezifischen Rechtsakten dürfen das Schutzniveau der DSGVO nicht unterlaufen.

**Datenportabilität und Datenmittler**: Erwogen wird, durch mehr Datenportabilitätsrechte für KonsumentInnen bzw einem Datenzugang für Mitbewerber die konzentrierte Marktmacht von Internetkonzernen zu brechen. Die Folge könnte sein, dass nur noch mehr Unternehmen Zugang zu Nutzerdaten haben.

Europäische Firmen könnten den exzessiven Datenverwertungspraktiken der großen Internetkonzerne nacheifern. Auch die Idee von Datentreuhändern dürfte den Wünschen der KonsumentInnen kaum entgegenkommen: sie müssen deren Seriosität, Kompetenz und Unabhängigkeit zunächst einmal vertrauen können, sonst drohen auf dieser Ebene neue Risiken des Datenmissbrauchs. KonsumentInnen haben wenig Bedarf, ihre Datenbestände von einem Dritten verwalten zu lassen, solange diese nicht auch Gewähr dafür leisten, dass diese datenschutzkonform sind und dies erforderlichenfalls auch durchsetzen.

**AK-Anliegen**: Die Marktwächterrolle haben in erster Linie Datenschutzbehörden und Verbraucherschutzvereine, die für ihre vielfältigen Aufgaben mehr Ressourcen benötigen.

### 1.2.2 Nicht personenbezogene Daten

Diese Daten sollen – so die Maxime – allen zugänglich sein: „Mit der zunehmenden Menge nicht-personenbezogener industrieller und öffentlicher Daten in Europa entsteht eine potenzielle Quelle für Wachstum und Innovation, die unbedingt genutzt werden sollte".
**Geräte- und Nutzungsdaten durch das Internet der Dinge**: Gegenstände, die ins Internet integriert sind, erlauben Firmen noch tiefere Einblicke in unser Leben – das Erstellen von Persönlichkeitsprofilen oder Prognosen über künftiges Verhalten inbegriffen. Die Entwicklung wirft zahlreiche (und trotz DSGVO) ungeklärte Fragen in Bezug auf die Privatsphäre auf: Wann weisen die Betriebsdaten vernetzter Geräte einen Personenbezug auf und wem gehören sie eigentlich? KonsumentInnen laufen Gefahr, dass ihr Selbstbestimmungsrecht über ihre Daten bzw ihr Eigentumsrecht an gekauften „smarten" Produkten nicht angemessen respektiert wird. So zeigte etwa eine Studie (https://www.arbeiterkammer.at/infopool/wien/Privatsphaere_in_Online-Spielen.pdf), dass populäre digitale Spiele nur mehr mit Onlineverbindung funktionieren, selbst wenn man sie alleine spielt. Ohne entsprechende Verbotsnorm dürften NutzerInnen smarter Geräte künftig noch oft gezwungen werden, dem Abgreifen ihrer Daten relativ machtlos zuzusehen. Insgesamt zeichnet sich ein krasses informationelles und vertragliches Ungleichgewicht in den Rechtspositionen zwischen den am Internet der Dinge beteiligten Anbietern und ihren Kunden ab.

Die Anbieterseite, nützt vertragliche und technische Gestaltungsmöglichkeiten, um personenbezogene Kundendaten und Betriebsdaten der Geräte zu analysieren und kommerziell zu verwerten, übernimmt wenig Verantwortung für immanente Risiken (Softwarefehler, Hackingangriffe, Databreaches, Insolvenzen mitbeteiligter Anbieter, schädigender Einsatz unausgereifter Algorithmen und Künstlicher Intelligenz) und investiert auch selten ausreichend in präventive Sicherheit.

**AK-Anliegen**: Ohne starke Intervention der Verbraucherpolitik dürften viele der offenen Fragen zu Datenschutz, Datensicherheit aber auch fairer Vertragsgestaltung ohne Rücksicht auf Verbraucherpositionen im Sinne der Hersteller beantwortet werden.
Auch falsche Ergebnisse und Schlussfolgerungen aus Datenauswertungen von Geräten, die auf dem Einsatz von Algorithmen und Künstlicher Intelligenz basieren, werden negative Auswirkungen auf KonsumentInnen haben. Ein adäquater Diskriminierungsschutz ist nicht in Sicht.

**DSGVO-Öffnungsklausel für Wissenschaft, Forschung, Statistik**: Art 89 eröffnet zum Nachteil der KonsumentInnen einen zu großen Spielraum, Betroffenenrechte auszuhebeln. Was eine wissenschaftliche Einrichtung überhaupt ist, ist nicht determiniert. Damit könnten sich selbst Internetriesen, die bspw Marktforschung betreiben, auf nationale Privilegien zugunsten von Wissenschaft und Forschung stützen. Es fehlt eine klare Grenze zu kommerziellen Aktivitäten.

**AK-Anliegen**: Damit die Freizeichnung von der DSGVO für Zwecke von Wissenschaft und Forschung in vertretbarem Rahmen bleibt, muss restriktiv definiert sein, wer die privilegierten Institutionen sind. Sollen Betroffenenrechte beschnitten werden, müssen Datenschutzbehörden eine Vorabprüfung durchführen. Im Zuge dessen ist zu bescheinigen, dass der Forschungsgegenstand im wichtigen öffentlichen Interesse liegt.

## 2. Marktspezifische Regulierung von digitalen Infrastruktureinrichtungen

Hinsichtlich der Schaffung klarer und fairer Regeln für den Datenzugang ist gerade bei den großen Plattformen jedenfalls auch eine marktspezifische Regulierung anzudenken, die es ermöglicht, ex-ante Mechanismen festzulegen, die einen diskriminierungsfreien Zugang zu Daten – soweit die datenschutzrechtlichen Schutzbestimmungen dies erlauben – gewährleisten. Dies ist – wie im Dokument der EU-Kommission ausgeführt – bereits in jenen Bereichen geschehen, wo Marktversagen festgestellt wurde, zB in der Automobilindustrie und bei Zahlungsdienstleistungen.

Es ist längst bekannt, dass große Onlineplattformen aufgrund ihrer Charakteristika zu Monopolen oder Oligopolen tendieren. Durch das Zusammenspiel verschiedener Mechanismen wie etwa Netzwerkeffekte, Skaleneffekte oder Lock-ins weisen große Internet-Plattformen Merkmale klassischer Infrastrukturen auf. Während klassische Infrastrukturen wie etwa das Stromnetz oder Schienennetze öffentlich reguliert sind, geben große Online-Plattformen die Regeln selbst vor und agieren als private Regelsetzer und „Gatekeeper".

Zahlreiche Fälle, die bis jetzt von den Wettbewerbsbehörden aufgegriffen wurden, deuten auch in diesem Bereich auf Marktversagen hin. Es ist nicht zu erwarten, dass die großen Internet-Plattformen wie Amazon, Google, Facebook, Uber, booking.com und Airbnb in absehbarer Zeit ihre überragende Marktstellung verlieren.

Die großen Internet-Plattformen verfügen demnach nicht nur über die wesentlichen technischen Infrastruktureinrichtungen („essential facilities") für digitale Dienste (Online-Handel, Online-Werbung, diverse Buchungsportale, Suchmaschinen, soziale Netzwerke), sondern sind auch im Besitz eines großen wettbewerbsrelevanten Datenpools. Diese große Datenmenge ist Voraussetzung für die Weiterentwicklung von digitalen Geschäftsmodellen und kann eine bereits starke Marktstellung der Unternehmen auch auf benachbarte Märkte übertragen.

Nach Ansicht der AK bedarf es für diese „großen Datensammler" auch einer ex-ante Regulierung, wie es auch die EU-Kommission bereits angedeutet hat.

Eine marktspezifische ex-ante Regulierung, welche zunächst jedenfalls für große Internet-Plattformen bzw marktmächtige Digitalunternehmen zur Anwendung kommen sollte, kann wesentliche Aufgaben zB bei Fragen des Datenzugangs, der Interoperabilität, der Datentransparenz und der Transparenz von Algorithmen bereits im Vorfeld einer Lösung zuführen.

Aber auch außergerichtlicher Streitbeilegung sollten vorgesehen werden und letztlich sollte auch eine Beschränkung einer exzessiven Datennutzung und Datenverknüpfung dann ins Auge gefasst werden, wenn ein massives Ungleichgewicht zwischen der Zurverfügungstellung von Daten und dem daraus resultierenden Datennutzen entstehen sollte.

## 3. Auch bei Cloud-Diensten Konzentrationstendenzen vorbeugen

Auch hinsichtlich der wachsenden Bedeutung von Cloud-Diensten sollte man die Fehlentwicklungen, die aus dem Wachstum der Plattform-Dienste bekannt sind, von vornherein in diesem Bereich vermeiden. Es ist unumgänglich, Konzentrationstendenzen vorzubeugen und Wettbewerb zu fördern und zuzulassen. Darüber hinaus ist dem Sicherheitsaspekt hohe Priorität einzuräumen. Insbesondere gilt es dabei auch, die Unabhängigkeit der europäischen Datenwirtschaft als kritische und sensible Infrastruktur gegenüber Dienstanbietern in Drittstaaten zu stärken und sich eine gewisse Autonomie zu bewahren.

## 4. Wettbewerbskonformer Zugang zu Daten

Unternehmen bzw Organisationen werden in der Konsultation auch befragt, ob sie bei der Nutzung von Daten anderer Unternehmen auf Schwierigkeiten gestoßen sind und welche Schwierigkeiten dies im Konkreten waren. Aufgezählt wurden sowohl die Weigerung des Datenzugangs oder unerschwingliche Preise.

Nach Ansicht der AK sollte die Auswertung dieser Frage auch zum Anlass genommen werden, bei Vorliegen von Schwierigkeiten beim Datenzugang auch wettbewerbliche Untersuchungen einzuleiten.

## 5. Datenwirtschaft und ArbeitnehmerInnenrechte

Die Menge der durch Datensammlung 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. Auch diesem Thema muss sich die europäische Datenstrategie verstärkt widmen und Schutzmechanismen ausarbeiten. Entscheidend dafür sind vor allem Mitbestimmungsrechte: Das können Informations-, Mitgestaltungs- und Zustimmungs- bzw Vetorechte der einzelnen Beschäftigten gegenüber Datenverarbeitungsanwendungen sein, aber vor allem auch – angesichts der Verhandlungsunterlegenheit der einzelnen Beschäftigten gegenüber dem Arbeitgeber – Informations-, Mitgestaltungs- und Zustimmungs- bzw Vetorechte von betrieblichen und überbetrieblichen Interessenvertretungen.

## 6. Abwägung der in Aussicht genommenen politischen Zielsetzungen

Letztendlich muss die EU-Kommission auch die von ihr verfolgten Politik-Ziele gegeneinander abwägen. Eine Forcierung des autonomen Fahrens zB könnte ohne geeignete Begleitmaßnahmen zu mehr Individualverkehr führen und so konträr zu der Zielsetzung Klimaschutz stehen.

Ebenso ist durch die verstärkte Nutzung von Datenströmen und Cloud-Diensten der zunehmende Aufbau von sehr energie- und ressourcenintensiven Rechenzentren und Serverfarmen zu erwarten. Aus diesem Grund müssen auch die Risiken und mögliche Auswirkungen auf die Umwelt weiter und intensiver thematisieret werden.

## 7. Breite Einbindung in den Diskussionsprozess

Bei jeder Technologieentwicklung – so auch in einer in der Bedeutung gewinnenden Datenwirtschaft – gibt es prinzipiell Gewinner und Verlierer. Nach Ansicht der AK müssen daher auch in diesem Bereich Abfederungsmaßnahmen ernsthaft diskutiert werden. Eine größtmögliche Beteiligung der Sozialpartner und der relevanten Akteure der Zivilgesellschaft ist dringend geboten und muss in den Vorhaben der Kommission auch so benannt und umgesetzt werden.

## Kontaktieren Sie uns!

**In Wien:**

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

**Ulrike Ginner**
T +43 (0) 1 501 651 2142
ulrika.ginner@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 (0) 2 230 62 54
alice.wagner@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.