Daniela Zimmer, Ulrike Ginner

AK-Positionspapier zum Data Governance Act aus Verbraucher- und Wettbewerbssicht

Dezember 2020

WIEN

GERECHTIGKEIT MUSS SEIN

AK-Positionspapier zum Data Governance Act aus Verbraucher- und Wettbewerbssicht

Der Rechtsakt regelt unter anderem:

- die kommerzielle Weiternutzung von Daten des öffentlichen Sektors, die aufgrund des Datenschutzes, geistiger Eigentumsrechte bzw Geschäftsgeheimnissen vor dem Zugriff Dritter eigentlich geschützt sind,
- Anmelderegeln für Unternehmen, die Daten gemeinsam nutzen wollen, für Datenvermittler, die als Treuhänder zwischen Privatpersonen und Datennutzern zwischengeschaltet sind und für Organisationen, die „gespendete" Daten „zum Wohl der Allgemeinheit" sammeln.

Zusammenfassende Bewertung des Entwurfes

Ein grundrechtlich äußerst sensibles Projekt

Die RL 2019/1024 „über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors" enthält bereits einen Rechtsrahmen für die innovative, kommerzielle Verwertung von Daten der öffentlichen Hand. Der Rechtsakt enthält allerdings noch die wesentliche Einschränkung, dass Rechte Dritter der Weiterverwendung nicht entgegenstehen dürfen. Mit dem vorliegenden Entwurf soll die Datenwirtschaft – unter Einhaltung einiger Anforderungen – auch auf geschützte Daten zugreifen können.

Mit anderen Worten: Daten, die aus Gründen des Datenschutzes, geistigen Eigentums bzw von Geschäftsgeheimnissen eigentlich unter Verschluss zu halten oder nur mit Einwilligung des Rechteinhabers nutzbar sind, können – müssen allerdings auch nicht – von öffentlichen Stellen zur Verfügung gestellt werden. Dass ein solches Vorhaben grundrechtlich überaus heikel ist, muss nicht näher erläutert werden. Umso bedachtsamer sind die flankierenden Schutzmaßnahmen aus BAK-Sicht zu wählen. Während die Förderung innovativer Datenbewirtschaftung überaus klar formuliert ist, sind die flankierenden Vorschriften, die die Rechte der Betroffenen absichern, unvertretbar vage.

Beurteilungsmaßstab

Für eine positive Bewertung des Vorhabens ist entscheidend, ob durch die Eröffnung des Zugangs zu geschützten Daten die Rechte Dritter weiterhin verlässlich geschützt sind. Nach unserer Einschätzung dürfte das nicht der Fall sein.

Versäumnisse

KonsumentInnen, PatientInnen, BürgerInnen usw können aus den folgenden Gründen den Datentransfers nicht ohne Weiteres vertrauen:

- keine konkreten Transparenz- und Datensicherheitspflichten für „öffentliche" bzw unterstützende „zuständige" Stellen und die Datenweiterverwender,
- keine Anonymisierungspflicht für öffentliche Stellen bevor sie Daten (ohne Zustimmung Betroffener) weitergeben,
- keine Vorgaben, wann Daten als verlässlich anonymisiert gelten,

- öffentliche Stellen werden kaum in der Lage sein, “die Ergebnisse der Datenverarbeitung zu prüfen und die Verwendung zu verbieten, wenn Infos enthalten sind, die die Interessen und Rechte Dritter gefährden“,

- keine spezifische Aufsichtsbehörde für derartige Datentransfers,
- keine klar abgegrenzten haftungsbegründenden Verantwortlichkeiten der einzelnen Akteure,
- kein niedrigschwelliger Rechtsschutz für Betroffene (Gerichtsweg steht offen, aber keine verwaltungsrechtliche Einspruchsmöglichkeit, Schlichtungsstelle etc). Betroffene werden sich gegen Geheimhaltungspflichtverletzungen so kaum erfolgreich wehren können.
- Der Mehrwert gewerblicher Aktivitäten von Datenmittlern, Datengenossenschaften und „datenaltruistischen“ Organisationen für ArbeitnehmerInnen, KonsumentInnen und BürgerInnen ist unklar. Angesichts dürftiger Ausübungsregeln überwiegt die Sorge vor Irreführung und Übervorteilung durch aggressives Marketing für derartige Dienste.
- Faire Wettbewerbschancen für kleine Unternehmen – etwa durch stärkere Regulierung großer „Datensammler“ – zählen bedauerlicherweise nicht zu den Zielen des Entwurfes.
- Die in engem Rahmen zulässigen Ausschließlichkeitsvereinbarungen dürfen aus diesem Grund keinesfalls mit den großen „Datensammlern“ abgeschlossen werden. Hierbei könnte man sich an jenen Unternehmen orientieren, die vom Digital Markets Act umfasst sein werden.

Eine Überarbeitung des Entwurfes ist daher zumindest in folgenden Punkten nötig

Vorbedingungen für die Förderung datengetriebener Wirtschaft sind nicht erfüllt

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 derzeit gesetzlich nicht geregelt.**

„Making more data available“ lautet die Devise. Wobei die EU-Kommission in ihrer Mitteilung zur EU-Datenstrategie betont, dass es der europäische Weg sei, „den Austausch und die breite Nutzung von Daten zu kanalisieren und **gleichzeitig hohe Datenschutz-, Sicherheits- und Ethikstandards** zu wahren“. Aus BAK-Sicht steht der Entwicklung zu einer Datenökonomie (jedenfalls 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 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 aber ein ehrliches Bekenntnis, dass manchmal nur eine „entweder oder"-Option besteht: kommerzielle Auswertung von großen Datenpools für unbestimmte Zwecke oder ein hohes Datenschutzniveau.

Die BAK fordert deshalb ein/e:

- **saubere Trennung zwischen (nicht) personenbezogenen Daten**: Der Vorschlag unterscheidet nicht präzise zwischen Daten mit und ohne Personenbezug (und ob es sich um besonders schützenswerte, sensible Daten handelt). Die Beurteilung, ob Schutzmaßnahmen ausreichen, hängt aber ganz wesentlich von der Kategorie der angesprochenen Daten ab. Dieses Defizit durchzieht den gesamten Entwurf. Wann personenbezogene Daten im Spiel sind, muss klar sein.
- **Informationspflicht der Betroffenen vor Datenweitergaben**: Bevor Daten, die sich im Besitz öffentlicher Stellen befinden, an Unternehmen weitergegeben werden, sind alle davon Betroffenen von der öffentlichen Stelle darüber über alle wichtigen Details zu informieren.
  Nur bei Kenntnis der Weitergabe können sie von ihren Rechten (Auskunft, Einspruch etc) Gebrauch machen.

- **Compliance-Stelle, mit klar abgegrenzter Verantwortung gegenüber öffentlichen Stellen:** Die öffentlichen Stellen sind von ihren Geheimhaltungspflichten nicht befreit (Art 3 Abs 3). Es soll aber „zuständige Stellen" geben (Art 7), die öffentliche Stellen bei der Bereitstellung der Daten, bei der Anonymisierung uÄ „unterstützen" oder selbst damit „betraut" sind, den Datenzugang zu gewähren. Damit kommen weitere Akteure ins Spiel, deren genaue Verantwortlichkeit ungeklärt ist. Wer wann und wofür im Zuge des Datentransfers bspw DSGVO-Verantwortlicher ist, ist im Entwurf unmissverständlich festzuschreiben.

- **klare Zuordnung der Verantwortung auch zwischen öffentlichen Stellen und den Datenweiterverwendern:** Eine Zuweisung, wer unter sämtlichen Akteuren für Datenschutzverstöße haftet, sucht man vergebens. Betroffene können sich gegen unzulässige Aktivitäten der Behörden und kommerziellen Datennutzer nur wehren, wenn sie wissen, wem gegenüber sie welche Ansprüche verfolgen können.

- **niedrigschwelliger Rechtsschutz:** Jeder Betroffene kann Entscheidungen der öffentlichen oder zuständigen Stellen vor Gericht bekämpfen (Art 8 Abs 4). Die Anordnung ist in eine Bestimmung eingebettet, die die „zentrale Informationsstelle" regelt und weist damit deutlich auf den geringen Stellenwert der Betroffenenrechte hin. Eine Auskunfts- und unabhängige Schlichtungsstelle sollte für Anfragen und Beschwerden interessierter wie besorgter BürgerInnen eingerichtet werden. Neben dem gerichtlichen Rechtsbehelf muss es Betroffenen auch möglich sein, einen kostenlosen Einspruch gegen Entscheidungen verwaltungsrechtlich einzubringen.

- **Aufsichtsbehörde als Kontrollorgan der Datentransfers:** Die öffentliche Stelle muss in der Lage sein, die Ergebnisse der Datenverarbeitung zu prüfen und die Verwendung zu verbieten, wenn Infos enthalten sind, die „die Interessen und Rechte Dritter gefährden" (Art 5 Abs 5). Behörden, die über Gesundheits-, Bildungs-, Finanz-, Mobilitätsdaten etc verfügen, dürften organisatorisch, rechtlich und technisch kaum in der Lage sein, die Datenverarbeitung von Unternehmen zu kontrollieren.

Auch die zuständige Stelle nach Art 7 unterstützt nur, hat aber keine Aufsichtsfunktion. Es bedarf einer behördlichen Aufsicht, die komplexe Kontrollaufgaben wahrnimmt.

- **Anonymisierung ausschließlich durch die öffentliche Stelle:** Öffentliche Stellen können (Art 5 Abs 3) „Verpflichtungen auferlegen, dass nur aufbereitete Daten weiterverwendet werden dürfen, sofern dadurch personenbezogene Daten anonymisiert oder pseudonymisiert werden." Welcher Akteur Anonymisierungen vorzunehmen hat, bleibt offen. In Verbindung mit Art 5 Abs 4 (Zugang von Unternehmen zu den Daten in sicherer Verarbeitungsumgebung bzw in bestimmten physischen Räumlichkeiten) besteht Anlass zu Sorge, dass Unternehmen Direktzugriff auf geschützte Daten erhalten, um sie „im sicheren Umfeld" einer Behörde selbst zu anonymisieren. Eine solche Vorgangsweise würde die BAK entschieden ablehnen.

  Ein grundrechtskonformer und vertrauenswürdiger Umgang setzt voraus, dass nur anonymisierte Daten die Behördenschnittstelle verlassen und Datennutzer erst nach der Anonymisierung darauf zugreifen können.

- **Verbot des Direkt- oder Fernzugriffs auf geschützte Daten (ohne Zustimmung der Betroffenen)**: Nach Art 5 Abs 4 können öffentliche Stellen den Zugang zu den Daten dahingehend einschränken, dass Zugang und Weiterverwendung in einem „vom öffentlichen Sektor bereitgestellten und kontrollierten sicheren Verarbeitungsumfeld oder innerhalb physischer Räumlichkeiten, in denen sich die sichere Verarbeitungsumgebung befindet, erfolgen muss." Die Kann-Bestimmung ist durch explizite Verbote zu ersetzen. Öffentliche Stellen dürfen aus BAK-Sicht keinen Fernzugriff auf geschützte Daten ohne vorherige Zustimmung der Betroffenen erlauben. Sie haben in diesem Fall Daten ausnahmslos in einem Zustand zu übergeben, der keine Rückführung auf eine individuelle Person erlaubt.

- **Verbot der Übermittlung geschützter Daten in Drittländer außerhalb der EU (ohne Zustimmung der Betroffenen):** Art 5 Abs 10 ist aus BAK-Sicht ersatzlos zu streichen. Demnach dürften öffentliche Stellen vertrauliche Daten nur dann einem Weiterverwender übermitteln, der Daten in ein Drittland ohne ein der EU entsprechendes Rechtsniveau übertragen will, wenn bestimmte vertragliche Verpflichtungen eingegangen werden. Aus BAK-Sicht dürfen aber öffentliche Stellen geschützte Daten ohne Zustimmung der Betroffenen Dritten gar nicht überlassen. Liegt eine Zustimmung des Betroffenen zur Weiterverwendung seiner Daten vor, so muss er auch frei darüber entscheiden können, ob er überhaupt einem Datentransfer in ein Drittland (insbesondere in ein Drittland ohne vergleichbares Datenschutzniveau) zustimmen möchte.

- **Festlegung, ab wann Daten als verlässlich anonymisiert gelten**: IT-ExpertInnen warnen, dass durch die Zusammenführung immer größerer Datenmengen und immer komplexere algorithmische Datenanalysen nicht mehr verlässlich bestimmt werden kann, ob Daten einen Personenbezug aufweisen. Vor einer großangelegten Weiternutzung von Daten dürfen sich EU-BürgerInnen diesbezüglich Rechtssicherheit erwarten.

Im Zuge der Evaluation „2 Jahre Datenschutz-Grundverordnung (DSGVO)“ wurde auf diese Säumnis von vielen Seiten hingewiesen. Wann gelten Daten als (hinreichend) anonymisiert? Welche Anonymisierungstechniken werden als Mindeststandard vorausgesetzt? Dürfen die Daten von niemandem mehr (oder nur bestimmten Subjekten) auf eine eindeutig bestimmte Person zurückgeführt werden können?
Kurz: Wer, wann, wie mit welcher Wahrscheinlichkeit vorgeblich anonyme Daten doch wieder auf einzelne Personen rückführen kann und wann deshalb noch (oder nicht mehr) von anonymen Daten die Rede sein darf, ist rechtlich ungeklärt. Für die BAK ist ein „Anonymisierungsgesetz“ zwingende Vorbedingung für grundrechtssensible Datenzugriffe.

Näheres zum Bedarf an einem „Anonymisierungsgesetz“

- Nach der **DSGVO** sollen „die Grundsätze des Datenschutzes für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. [...] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.“ Wann ein Personenbezug vorliegt, ist demnach keine triviale Frage. Unzählige Fachkommentare befassen sich mit der Grenzziehung zwischen anonymen und indirekt personenbezogenen Daten und kommen oft zu keinem einhelligen Ergebnis. Gewarnt wird zudem davor, dass durch die Entwicklung von Deanonymisierungstechniken vormals anonyme Daten in Zukunft einen Personenbezug aufweisen könnten.

- Zur Illustration sei auf das **Sachverständigengutachten für den Deutschen Bundestag** verwiesen: „Wie wird der Begriff der Verkehrs- und Nutzungsdaten wissenschaftlich im technischen und juristischen Kontext gebraucht? Wie ist dieser vom Begriff der Metadaten abzugrenzen?" (https://dipbt.bundestag.de/doc/btd/18/CD12850/D_II_Sachverstaendigengutachten/31%20Gutachten%20Dr.%20Boehm%20und%20Dr.%20B%C3%B6hme.pdf
Demnach sei „*in einem ersten Schritt zu klären, ob überhaupt jemand den Personenbezug herstellen kann. Ist es objektiv ausgeschlossen, dass der Betroffene bestimmt werden kann, fehlt es am Personenbezug. Eine solche Situation, in der nicht einmal ein Dritter existiert, der den Personenbezug vornehmen kann, dürfte jedoch relativ selten sein.*

  Ganz im Gegenteil lässt die ständig steigende Vielfalt hochkomplexer Auswertungsmechanismen und deren einfache Verfügbarkeit faktisch die Anzahl derjenigen Stellen steigen, die in der Lage sind, zwischen gespeicherten Angaben und einer natürlichen Person einen Bezug herzustellen. In diesem Zusammenhang ist es gleichermaßen von Bedeutung, dass die Quantität der Daten ansteigt und die Nachfrage danach ebenso zunimmt.“

- Sofern die Möglichkeit der Bestimmbarkeit nicht objektiv ausgeschlossen ist, weil ein Dritter einen Personenbezug herstellen kann, kommt es laut **EuGH** auf die Mittel an, die zur Bestimmbarkeit genutzt werden können. Ganz konkret stellten die Richter im **Fall Breyer (C-582/14)** die Frage, ob für die verantwortliche Stelle vernünftige Mittel bestehen, um die für die Zuordnung notwendige Information vom Dritten zu erhalten.
Ihrer Ansicht nach kommt es also ausdrücklich nicht darauf an, dass sich *„alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen [des für die Daten Verantwortlichen] befinden“.*

Was in diesem Zusammenhang „vernünftige Mittel" sind, wurde vom EuGH offengelassen. Es erfolgte lediglich eine negative Abgrenzung*: „Mittel, die nicht vernünftigerweise eingesetzt werden können und die deshalb bei der Bestimmung des Personenbezugs unberücksichtigt bleiben müssen, sind solche, deren Nutzung zur Identifizierung gesetzlich verboten ist oder mit denen die Identifizierung praktisch nicht durchgeführt werden kann."*

- Auch das aktuelle **Regierungsübereinkommen** der österreichischen Bundesregierung nimmt sich vor, Kriterien für eine vertrauenswürdige Anonymisierung von Daten festzulegen.

- **Berücksichtigung des Risikos einer erneuten Identifizierung betroffener Personen anhand anonymisierter Daten**: Diese Anforderung in Art 5 Abs 11 bezieht sich unverständlicherweise nur auf Datenübertragungen in Drittländer. Vorkehrungen und Beschränkungen gegen eine rechtswidrige Aufhebung der Anonymisierung müssen natürlich auch getroffen werden, wenn die Daten in der EU zirkulieren.

- **Konkretisierung, wie die wichtigsten DSGVO-Grundsätze bei Datentransfers umzusetzen sind:** Ein lapidarer Verweis, dass der Entwurf die DSGVO unberührt lässt, reicht keinesfalls. Maßgeschneiderte Datenschutz- und Datensicherheitsmaßnahmen, die den Risiken eines Datentransfers zwischen öffentlichen Stellen und Unternehmen angemessen sind, fehlen. Der Entwurf sollte herausarbeiten, wie die wichtigsten DSGVO-Prinzipien mit Zugriffsrechten in Einklang zu bringen sind. Dazu zählen bspw: Datensparsamkeit, Zustimmungserfordernis zur Datennutzung in Kenntnis der exakten Verarbeitungszwecke, Verbot der Weiterverarbeitung zu mit dem Ursprungszweck nicht vereinbaren Zwecken usw. Die DSGVO setzt der Weiterverwendung von personenbezogenen Daten jedenfalls enge Grenzen. In der Regel dürften deshalb nur verlässlich anonymisierte Daten im Datenpool landen, um für innovative Geschäftsideen weiterverarbeitet zu werden. Nach Art 5 Abs 6 sollen öffentliche Stellen potentielle Datennutzer beim Einholen von Zustimmungen unterstützen. Die Rollenverteilung muss im Entwurf klargestellt werden: wer informiert nach Art 12ff DSGVO, erteilt Auskünfte nach Art 15 DSGVO, wer protokolliert welche Vorgänge und nimmt den Widerruf bereits erteilter Zustimmungen entgegen?

- **Vorabkontrollpflicht von Datenschutzbehörden bei Anwendungen, die der Folgenabschätzung nach der DSGVO unterliegen**: Betroffene möchten Vorsorge statt hinterher das Nachsehen und bloße Schadenersatzansprüche zu haben. Um dem deutlichen Expertenruf nach einer Vorabkontrolle der „Fairness" von Algorithmen zu entsprechen, braucht es künftig ohnehin mehr behördliche Prüfungen 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 Schaden anrichten.

- **klare Ausübungsregeln für Datenmittler:** Art 9 führt das anmeldepflichtige Gewerbe des Datenvermittlungsdienstes ein. Er soll als Drehscheibe zwischen Personen, „die ihre personenbezogenen Daten zugänglich machen wollen" und potentiellen Datennutzern fungieren. Dabei wird auf die DSGVO vage Bezug genommen. Welche Services ein Datenmittler gegenüber KonsumentInnen als vertraglichen Mindestinhalt zu erbringen hat, bleibt offen. Auch aus den Anforderung gegen Betrug, Missbrauch und zugunsten von Datenschutz und - sicherheit in Art 11 lässt sich nicht ableiten, womit KonsumentInnen Datenmittler beauftragen können.

Ein Mehrwert wäre es, wenn die Prüfung der DSGVO-Konformität von Diensten, die der Konsument nutzen möchte, und widrigenfalls die Rechtsdurchsetzung zu den Mindestvertragsinhalten zählen würde. Dabei handelt es sich letztlich um ein anwaltliches Aufgabenfeld und damit nichts signifikant Neues.

- **klare Ausübungsregeln für Datengenossenschaften:** Sie sind ebenfalls anmeldepflichtig, handeln „zur Unterstützung betroffener Personen" vor deren Einwilligung die Bedingungen der Datenverarbeitung aus und stellen dazu „Mechanismen für den Meinungsaustausch" bereit, um den „Interessen der betroffenen Personen am besten gerecht zu werden". Wie ein derartiges Kollektiv zu rechtsverbindlichen Beschlüssen gelangt, sprengt jede Vorstellungskraft. Außer einer schwer verständlichen Definition des Begriffes stellt der Entwurf nichts Erhellendes bereit.

- **klare Aufgabenzuweisung an die Aufsichtsbehörden:** Für Datenmittler und Datengenossenschaften sind eine Vielzahl an Behörden zuständig: die Behörde für die Anmeldung, Datenschutz-, Wettbewerbs,- Cybersicherheit und andere „einschlägige Fachbehörden" (Art 12 und 13). Wer angesichts überschneidender Themenfelder wofür genau verantwortlich ist, lässt der Entwurf offen.

- **mehr Schutz gegenüber „datenaltrustischen Organisationen":** Außer Registrierungspflichten (samt Entzugsmöglichkeiten) gibt es wenig Schutzelemente gegen die Gefahr der Übervorteilung und Ausnutzung der Leichtgläubigkeit von KonsumentInnen. Dateninhaber müssen nach Art 19 von den registrierten Organisationen etwas über „die Zwecke von allgemeinen Interesse und etwaige Verarbeitungen außerhalb der Union" erfahren. Derartige Infofragmente erfüllen nicht die DSGVO-Anforderungen an Information und Einwilligung. Es ist Vorsorge zu treffen, dass nicht mit aggressiven, irreführenden Marketingpraktiken (zB Erschleichen von Gesundheitsdaten zur vermeintlichen Rettung Kranker, Gewinnversprechen etc) für Datenspenden geworben wird. Derartige Einrichtungen sollten nicht anders behandelt werden als gewerbliche Datenmittler. Darüber hinaus sind verwaltungsbehördliche Sanktionsmechanismen vorzusehen, wenn unrichtige Behauptungen aufgestellt werden, eine anerkannte datenaltruistische Organisation zu sein.

Der direkte Weg zu unseren Publikationen:
E-Mail: konsumentenpolitik@akwien.at

Impressum

Medieninhaber: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Zulassungsnummer: AK Wien 02Z34648 M
AuftraggeberInnen: AK Wien, Konsumentenpolitik
Autorin: Daniela Zimmer, Ulrike Ginner
Grafik Umschlag und Druck: AK Wien
Verlags- und Herstellungsort: Wien

Stand Dezember 2020
Im Auftrag der Kammer für Arbeiter und Angestellte für Wien

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Downloaden:

wien.arbeiterkammer.at/service/studien

AK WIEN