Digital Autonomy Hub
Technik souverän nutzen

POLICY BRIEF #1
Dezember 2020

Data Trusts

Personenbezogene Daten selbstbestimmt teilen – geht das?

Digital Autonomy Hub

Inhalt

DATA TRUSTS: PERSONENBEZOGENE DATEN SELBSTBESTIMMT TEILEN – GEHT DAS?

Wie lassen sich personenbezogene Daten für das Gemeinwohl nutzen, ohne die individuelle Selbstbestimmung zu untergraben? In unserem Policy Brief fragen wir, ob die in letzter Zeit oft diskutierte Idee der „Data Trusts“ eine Antwort auf diese Herausforderung sein kann und welche (rechtlichen) Voraussetzungen geschaffen werden müssten, um Data Trusts in Deutschland einzurichten. Der erste Schritt: die Datenschutz-Grundverordnung (DSGVO) anpassen.

Als im Juni 2020 die Corona-Warn-App in Deutschland eingeführt wird, sind die Erwartungen groß: Sie soll helfen, Übertragungswege schneller und präziser zu verfolgen, Infektionsketten frühzeitig zu erkennen und Bürger·innen gezielt zu warnen. Kontaktbegegnungen systematisch zu erheben und auszuwerten soll dabei helfen, die COVID-19-Pandemie einzudämmen. Gleichzeitig ist klar: Der Erfolg der App hängt wesentlich davon ab, ob die Bürger·innen darauf vertrauen, dass die App tut, was sie verspricht. Nur wenn sehr viele Menschen die App nutzen und bereit sind, Testergebnisse zu teilen, lässt sich das Potenzial der App voll ausschöpfen. Führende Politiker·innen appellieren an den Gemeinsinn: Mit der App könne jede·r Bürger·in einen wichtigen Beitrag dazu leisten, die Pandemie zu bekämpfen und die öffentliche Gesundheitsversorgung aufrechtzuerhalten.

Fünf Monate später haben fast 22 Millionen Menschen die Corona-Warn-App heruntergeladen.[1] Umfragen lassen darauf schließen, dass ein Großteil der Nutzer·innen durch die Verwendung der App das Gefühl hat, einen wichtigen gesellschaftlichen Beitrag zu leisten.[2] Einige empfinden die Nutzung der App gar als ihre gesellschaftliche Pflicht.[3] Gleichzeitig stößt die Corona-Warn-App weiterhin bei vielen Bürger·innen auf Skepsis. Obwohl die App von Expert·innen, wie dem Chaos Computer Club, als datenschutzfreundlich eingestuft wird, bezweifeln viele, dass die Daten ausreichend geschützt sind; sie fürchten Datenmissbrauch und Eingriffe in ihre Selbstbestimmung.[4]

1 Stand 6.11.2020, RKI (2020): https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_06112020.pdf?__blob=publicationFile.

2 Initiative D21 (2020): Corona-Warn-App: Einstellungen und Akzeptanz der Bevölkerung. Vorabergebnisse aus dem eGovernment MONITOR 2020. Unter: https://initiatived21.de/app/uploads/2020/09/ergebnisse-befragung-corona-warn-app-egovernment-monitor-2020-1.pdf; vgl. Bitkom (2020): https://www.bitkom.org/Presse/Presseinformation/28-Millionen-wollen-Corona-Warn-App-dauerhaft-nutzen.

3 In einer Umfrage im Auftrag von Bitkom empfanden 40% der befragten App-Nutzer die Verwendung der App als ihre gesellschaftliche Pflicht. Unter: https://www.bitkom.org/Presse/Presseinformation/28-Millionen-wollen-Corona-Warn-App-dauerhaft-nutzen.

4 In einer Umfrage im Auftrag der Gesellschaft zu Förderung der Unterhaltungselektronik (gfu) bezweifelten ein Drittel (33%), dass die Daten ausreichend geschützt sind; knapp ein Drittel (30%) befürchtete Eingriffe in die Selbstbestimmung. 48% der Befragten gaben an, die App-Nutzung habe keinen persönlichen Mehrwert. Unter: https://www.zeit.de/news/2020-09/02/jeder-zweite-will-corona-warn-app-nicht-installieren. Ein ähnliches Bild zeigen die Vorabergebnisse aus dem eGovernment MONITOR 2020 zur Corona-Warn-App in Deutschland: Im August äußerte die Hälfte der Befragten (51%). Sorge, dass seine/ihre Daten aus der App auch für andere Zwecke missbraucht werden. Knapp die Hälfte der Befragten (44%) fürchtete durch die App zu viel Überwachung durch den Staat. Unter: https://initiatived21.de/app/uploads/2020/09/ergebnisse-befragung-corona-warn-app-egovernment-monitor-2020-1.pdf.

DATEN ZUM WOHLE ALLER TEILEN UND SELBSTBESTIMMUNG WAHREN

Das zwiespältige Verhältnis der Bürger·innen zur Corona-Warn-App zeigt ein grundlegendes Dilemma auf: Einerseits verspricht es enorme Erkenntnisgewinne von gesellschaftlichem Nutzen, wenn personenbezogene Daten systematisch erhoben und ausgewertet werden können, etwa um die Ausbreitung einer Epidemie besser zu verstehen und besonders gefährdete Menschen zu schützen. Andererseits empfinden viele Menschen großes Unbehagen und Misstrauen, wenn es darum geht, sensible Daten weiterzugeben.

Große Datenmengen zu analysieren kann dabei helfen, gesellschaftliche Herausforderungen zu bewältigen. Standortdaten in Echtzeit auszuwerten kann eine effizientere und umweltschonendere Verkehrsführung ermöglichen; unzählige medizinische Studien und anonymisierte Befunde systematisch zu vergleichen kann dabei helfen, personalisierte Therapiemöglichkeiten zu entwickeln. Es mehren sich daher die Rufe, den „Datenschatz“ nicht länger nur profitorientierten Unternehmen zu überlassen, sondern gezielt für das Gemeinwohl zu nutzen. Die Europäische Kommission hat dafür Ende November eigens ein neues Gesetz zum Datenmanagement („Data Governance Act“, kurz: DGA) vorgeschlagen. Explizites Ziel des DGA: Instrumente zu schaffen, die die Nutzung von Daten aus altruistischen Gründen ermöglichen.[5] In ein ähnliches Horn stoßen die beiden SPD-Politikerinnen Esken und Korkmaz-Emre, die kürzlich eine „Kultur des Daten-Teilens“ zum Wohle aller gefordert haben.[6] Beide Vorschläge lassen allerdings die Frage unbeantwortet, wie das mit personenbezogenen Daten möglich sein soll.

Eine „Kultur des Daten-Teilens“, insbesondere wenn es um personenbezogene Daten geht, setzt Vertrauen voraus. Doch viele Menschen empfinden großes Unbehagen und Misstrauen, wenn es um die Bereitstellung sensibler Daten geht. Erst recht, wenn sie das Gefühl haben, die Verfügungsgewalt über diese Daten zu verlieren und in ihrer Selbstbestimmung eingeschränkt zu werden. Paradoxerweise haben ausgerechnet das Recht auf informationelle Selbstbestimmung und die Datenschutz-Grundverordnung (DSGVO) nicht unwesentlich dazu beigetragen, dass heutzutage ein Gefühl von Machtlosigkeit, Kontrollverlust und Misstrauen im

5 Europäische Kommission (2020): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz). COM(2020) 767 final. 25.11.2020. S. 1. Unter: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.

6 Esken und Korkmaz-Emre (2020): Digitaler Fortschritt. Daten sind Macht und müssen dem Gemeinwohl dienen. Unter: https://www.handelsblatt.com/meinung/gastbeitraege/gast-kommentar-digitaler-fortschritt-daten-sind-macht-und-muessen-dem-gemeinwohl-dienen/26572380.html?ticket=ST-12286226-beKGbPtjfd136tlf1LHr-ap4.

Umgang mit Daten vorherrscht.[7] Jede noch so triviale Datenverarbeitung bedarf der Zustimmung der Einzelnen und führt zu komplizierten Einwilligungs- und umfangreichen Datenschutzerklärungen, die für Nichtjurist·innen kaum verständlich sind. Anschauliches Beispiel sind die sogenannten Cookie-Banner, die Web-Nutzer·innen letztendlich nur darin trainieren, sie möglichst schnell wegzuklicken und abzunicken. Die „informierte und freiwillige Zustimmung" wird ad absurdum geführt.

Im Fall der Corona-Warn-App bewirken die starken Datenschutzvorkehrungen beispielsweise, dass die App-Nutzer·innen Daten, die sie selbst zur Verfügung gestellt und erzeugt haben, nicht selbst ansehen können. Sie füttern ein System, aber haben keinerlei Einblick in, geschweige denn Einfluss auf die Verarbeitung ihrer Daten. Digitale Bevormundung statt Selbstbestimmung.

Wer es ernst damit meint, „Big Data" für das Gemeinwohl nutzbar zu machen, muss sich diesem Spannungsverhältnis von Datenschutz und digitaler Selbstbestimmung stellen. Wir müssen uns über Ansätze unterhalten, die einen möglichen Ausweg aus der Sackgasse aufzeigen, die Vertrauen schaffen und Selbstbestimmung fördern.

7 Die deutsche Datenethikkommission spricht von einer „systematischen Überforderung des Einzelnen" aufgrund „der Anzahl und Komplexität der ihm abverlangten Entscheidungen bezüglich einer datenschutzrechtlichen Einwilligung ebenso wie durch die Unabschätzbarkeit aller Auswirkungen einer Datenverarbeitung". Datenethikkommission (2019): Gutachten. S. 96. Unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

LÖSUNGSANSATZ: DATA TRUSTS

Ein in letzter Zeit intensiv diskutierter Ansatz ist der sogenannte Data Trust, meist mit „Datentreuhänder" übersetzt.[8] In Deutschland empfehlen die Datenethikkommission, wie auch die Kommission Wettbewerbsrecht 4.0. und die Enquete-Kommission Künstliche Intelligenz, die Einrichtung von Datentreuhändern zu untersuchen, angesichts ihres Potenzials, „die Verbesserung der persönlichen Kontrolle über Daten und die Verbesserung des Datenzugangs in Einklang zu bringen".[9] Die Bundesregierung hat in ihren „Eckpunkten einer Datenstrategie" angekündigt zu analysieren, ob und wie Datentreuhänder das freiwillige Teilen von Daten stärken können.[10] Auf EU-Ebene greift die Kommission die Idee vom vertrauenswürdigen Datenmittler im Rahmen des DGA auf.[11]

8 Hinter dem Begriff „Datentreuhänder" verstecken sich allerdings eine Vielzahl von Konzepten und Modellen, die sich teils stark in Ziel und Anwendungsmöglichkeiten unterscheiden. Oft wird auch von Personal Information Management Systems (PIMS) oder Datenintermediären als Unterkategorien von Datentreuhändermodellen gesprochen. Für eine Diskussion der Begriffe vgl. Verbraucherzentrale Bundesverband (2020): Neue Datenintermediäre. Unter: https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf.

9 Deutscher Bundestag (2020). Unterrichtung der Enquete-Kommission Künstliche Intelligenz. Vorabfassung. S. 56. Unter: https://dip21.bundestag.de/dip21/btd/19/237/1923700.pdf; vgl. Gutachten der Datenethikkommission (2019). S. 22. Unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6; vgl. Kommission Wettbewerbsrecht 4.0 (2020): Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. S.43. Unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=12.

10 Bundesregierung (2019): Eckpunkte einer Datenstrategie der Bunderegierung. S. 3. Unter: https://www.bundesregierung.de/resource/blob/997532/1693626/e617eb58f3464ed13b8ded65c7d3d5a1/2019-11-18-pdf-datenstrategie-data.pdf.

11 Europäische Kommission (2020): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz). COM(2020) 767 final. 25.11.2020. S 1. Unter: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.

DATA TRUSTS IN DER PRAXIS

Das Datentreuhändermodell, mit dem wir uns in diesem Policy Brief befassen, entspringt der angelsächsischen Rechtsfigur des „Trusts“, in dessen Zentrum eine rechtlich verbindliche Treue- und Sorgfaltspflicht steht. Die Idee: Eine natürliche oder juristische Person („Data Trust“), verwaltet für jemand anderen („Datengeber·in“) Daten bzw. Rechte in Bezug auf diese Daten und stellt diese Dritten („Datennutzer·in“) zur Nutzung zur Verfügung. Dabei muss der Data Trust, ausgehend von der rechtsverbindlichen Treue- und Sorgfaltspflicht, stets und ausschließlich im Interesse der Datengeber·innen handeln, kann aber agieren, ohne dass ständig deren Mitwirkung erforderlich wäre.[12]

Der Vorteil für Datengeber·innen: Statt Entscheidungen selbst treffen zu müssen – im Zweifel überfordert und uninformiert –, wird die Entscheidungsgewalt anderen übertragen, die über die nötige Expertise und Ressourcen verfügen, die Interessen der Datengeber·innen optimal gegenüber den Datennutzer·innen zu vertreten.

Das klingt erst einmal gut, setzt aber einiges voraus:

1. die Datengeber·innen müssen fähig sein, einen geeigneten Data Trust zu identifizieren;

2. es muss sichergestellt werden, dass der Data Trust auch wirklich seiner Treuepflicht nachkommt;

3. die Datengeber·innen müssen den Data Trust stets über ihre Interessenlage informiert halten, die sich möglicherweise mit der Zeit ändert.

Wie können wir uns das in der Praxis vorstellen? Welche Anforderungen entstehen daraus? Und welche (rechtlichen) Voraussetzungen müssen dafür geschaffen werden?

Data Trusts sind zwar in aller Munde – Praxiserfahrungen oder Vorschläge, wie sie konkret ausgestaltet und umgesetzt werden können, gibt es jedoch kaum.[13] Behelfen wir uns mit einem kleinen Gedankenexperiment:

Eine Person, möglicherweise selbst auf medizinische Unterstützung angewiesen, möchte einen Beitrag zur medizinischen Forschung leisten und ist grundsätzlich bereit, ihre medizinischen Daten und Untersuchungsbefunde zu teilen. Die Freigiebigkeit ist allerdings an Bedingungen geknüpft: Die Datenauswertung soll ausschließlich gemeinwohlorientierter Forschung zugutekommen und nicht von Pharmaunternehmen kommerzialisiert werden. Ferner sollen aus der Datenauswertung keine Rückschlüsse auf den/die Datenspender·in gezogen werden können. Und schließlich möchte die Person nachvollziehen können, wie die Daten verwendet und welche Rückschlüsse daraus gezogen werden.

Die Person stößt auf die vielversprechende Studie einer renommierten öffentlichen Forschungseinrichtung, für die noch Studienteilnehmer·innen gesucht werden. Um an der Studie teilnehmen zu können, muss die Person eine dreißigseitige Einverständniserklärung unterschreiben. Die Forschungseinrichtung möchte sich absichern, dass sie keine Datenschutzvorschriften verletzt. Die Person verfügt allerdings weder über das medizinische noch das juristische Wissen, die nötig sind, um die Erklärung zu verstehen

12 Funke (2020): Gutachten: Die Vereinbarkeit von Data Trusts mit der DSGVO. Unter: https://algorithmwatch.org/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf

13 Blankertz (2020): Designing Data Trusts. Why We Need to Test Consumer Data Trusts Now. https://www.stiftung-nv.de/en/publication/designing-data-trusts-why-we-need-test-consumer-data-trusts-now#collapse-newsletter_banner_bottom. Erste Vorschläge bietet das kürzlich erschienene Positionspapier des Bundesverbands der Verbraucherzentrale zu Datenintermediären: https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf

und eine informierte Entscheidung zu treffen. Werden die drei Bedingungen erfüllt? Ist die Teilnahme in ihrem Interesse? Sie wünscht sich die Einschätzung von Expert·innen, denen sie voll und ganz vertraut. Doch in ihrem Familien- und Freundeskreis gibt es niemanden mit dieser Expertise.

Die Person macht sich daher auf die Suche nach vertrauenswürdigen Datentreuhändern im Gesundheitssektor und stößt auf eine Vielzahl an Anbietern und Einrichtungen. Leicht überfordert von der Situation schließt die Person zunächst alle Anbieter aus, die möglicherweise ein finanzielles oder anderweitiges Interesse an der Verwertung der Daten haben. Die potenziellen Datentreuhänder sollen unabhängig und neutral sein. Es verbleiben eine Handvoll Anbieter – Genossenschaften, öffentlich-rechtliche Einrichtungen und Stiftungen.

Anschließend versucht die Person, all jene Anbieter auszuschließen, die möglicherweise organisatorisch, technisch oder fachlich nicht in der Lage sind, die beste Entscheidung in ihrem Interesse zu treffen. Da die Person selbst nicht in der Lage ist, das zu bewerten, und es auch keine gesetzlichen Mindeststandards gibt, wer sich „Datentreuhänder“ nennen darf, orientiert sich die Person an Prüfsiegeln und Zertifikaten von Trägern, denen sie aus Erfahrung vertraut. Wichtig ist der Person dabei, dass das Prüfsiegel ein glaubwürdiges Kontroll- und Sanktionssystem der Datentreuhänder umfasst. Der Kreis der infrage kommenden Datentreuhänder schrumpft weiter.

Die verbleibenden Anbieter ordnet die Person schließlich nach Teilhabemöglichkeiten. Welche (Steuerungs-)Strukturen ermöglichen es ihr am besten, ihre – sich möglicherweise ändernden – Interessen zu äußern, an Grundsatzentscheidungen teilzuhaben und nachzuvollziehen, wie die Daten verwertet werden? Anbieter, die (direkt-)demokratisch geführt werden und leicht verständliche Berichte über die Datenverwendung zur Verfügung stellen, machen das Rennen.

Am Ende dieses Prozesses ist die Person zwar völlig erschöpft, aber hat einen Datentreuhänder gefunden, dem sie nicht nur die Entscheidung über die Studieneinwilligung anvertraut, sondern auch, ihre Gesundheitsdaten anderen Projekten zur Verfügung zu stellen, die den eingangs aufgestellten Kriterien entsprechen. Die aufwändige Suche nach geeigneten Datentreuhändern muss sich schließlich längerfristig auszahlen.

Das gefundene Arrangement ist aber nicht nur aus Sicht der Person komfortabel und eine Möglichkeit, Daten selbstbestimmt dem Gemeinwohl zur Verfügung zu stellen, sondern auch aus Sicht der Forschungseinrichtung. Die von der Person bereitgestellten Daten und deren Auswertung sind vermutlich nicht nur für diese eine Studie interessant, sondern auch für weitere, zukünftige Forschungsvorhaben. Müsste die Einrichtung nun jedes Mal von allen Datenspender·innen eine neue dreißigseitige Einverständniserklärung einholen, ginge dies mit einem gehörigen administrativen Aufwand und entsprechenden Kosten einher. Stattdessen kann sie mit Datentreuhändern kooperieren, die die Interessen vieler Datenspender·innen bündeln.

Das skizzierte Szenario ist ein Gedankenexperiment und bildet nur einen möglichen Anwendungsfall ab. Es verdeutlicht aber, welche Voraussetzungen nötig sind, damit Data Trusts helfen können, personenbezogene Daten selbstbestimmt dem Gemeinwohl zur Verfügung zu stellen. Es müsste ein gesetzlicher Rahmen geschaffen werden, der es Personen möglichst leicht macht, einen geeigneten Data Trust zu finden, denen sie vertrauen. Oder, um bei dem obigen Beispiel zu bleiben: Niemand sollte am Ende der Suche völlig erschöpft sein. Es wäre zu prüfen, inwieweit gesetzliche Mindeststandards, das Schützen des Begriffs „Datentreuhänder" sowie die Förderung glaubwürdiger und leicht verständlicher Prüfsiegel dazu einen Beitrag leisten können. Dabei könnten sich politische Entscheidungsträger·innen an folgenden Kriterien für Datentreuhänder orientieren: (1) Unabhängigkeit und Neutralität, (2) organisatorische und technische Kapazität, (3) fachliches Wissen, (4) Kontroll- und Sanktionsmechanismen und (5) Teilhabemöglichkeiten.

DATA TRUSTS RECHTSSICHER EINRICHTEN

Das obige Gedankenexperiment setzt voraus, dass es überhaupt möglich ist, das Recht zu übertragen, personenbezogene Daten zu verarbeiten und Betroffenenrechte wahrzunehmen. Ein kürzlich von AlgorithmWatch in Auftrag gegebenes Rechtsgutachten kommt allerdings zu dem gegenteiligen Schluss: Derzeit erlaube es die DSGVO nicht, derartige Data Trusts rechtssicher in Deutschland einzurichten: „Eine Übertragung des Rechts, Verarbeitungen zu gestatten, Betroffenenrechte oder andere Abwehrrechte wahrzunehmen, ist unter der DSGVO nicht möglich."[14] Ferner seien rechtlich vertretbare Stellvertretungslösungen aufgrund der strittigen Rechtslage mit signifikanten Rechtsunsicherheiten verbunden. Das erklärt, warum es bisher an Praxisbeispielen zu Data Trusts mangelt – zu groß ist die Rechtsunsicherheit. Auch der Data Governance Act schafft hier keine Klarheit, denn er lässt die Regelungen der DSGVO unangetastet.

Der erste Schritt müsste daher sein, die DSGVO anzupassen. Das Gutachten macht dazu konkrete Vorschläge[15]: Der europäische Gesetzgeber könnte in der DSGVO eine neue Figur neben „Verantwortlichem" und „Auftragsverarbeiter" schaffen, die die Rechte der betroffenen Person innehaben und wahrnehmen kann. Ihr können damit nicht nur Rechte übertragen, sondern auch Pflichten zugeschrieben und damit Mindeststandards etabliert werden. Eine weitere Möglichkeit bestünde darin, in der DSVGO explizit die Möglichkeit einer Stellvertretung zu schaffen und diese auszubauen. Schließlich, quasi als Minimallösung, könnten Aufsichtsbehörden, wie der europäische Datenschutzausschuss, bestehende Rechtsunsicherheiten mittels eindeutiger Positionierungen zumindest vermindern.

Der zweite Schritt muss sein, verschiedene Modelle eines Data Trusts in der Praxis zu testen. Wie allgemein oder spezifisch sollte ein Data Trust gefasst sein? Welche Anwendungsbereiche sind geeignet? Welcher Form der Trägerschaft und Aufsicht würden Bürger·innen vertrauen? Befriedigende Antworten auf diese Fragen werden wir erst finden, wenn wir Modelle in der Praxis testen.

14 Funke (2020): Gutachten: Die Vereinbarkeit von Data Trusts mit der DSGVO. S. 5. Unter: https://algorithmwatch.org/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf.

15 Funke (2020): Gutachten: Die Vereinbarkeit von Data Trusts mit der DSGVO. S. 6. Unter: https://algorithmwatch.org/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf.

Digital
Autonomy Hub
Technik souverän nutzen

Der *Digital Autonomy Hub – Technik souverän nutzen* ist ein Kompetenzzentrum, das ein interdisziplinäres Netzwerk von 43 Instituten und Organisationen koordiniert. Der Hub macht sichtbar, woran die Partner forschen und welche Ideen sie entwickeln, um die individuelle digitale Souveränität zu stärken. Ziel dieses Wissenstransfers ist es, allen Menschen einen reflektierten und selbstbestimmten Umgang mit ihren Daten, Geräten und Anwendungen zu ermöglichen. Das Kompetenzzentrum bereitet aktuelle Forschungsergebnisse für Zivilgesellschaft, Politik, Wissenschaft und Wirtschaft auf und berät die verschiedenen Akteure zu ethischen, rechtlichen und sozialen Aspekten der Datennutzung.

Der *Digital Autonomy Hub* wird vom Bundesministerium für Bildung und Forschung im Rahmen des Forschungsprogramms „Technik zum Menschen bringen" gefördert und von AlgorithmWatch und Gesellschaft für Informatik e.V. (GI) umgesetzt.

Mehr Informationen unter: www.digitalautonomy.net

Data Trusts: Personenbezogene Daten selbstbestimmt teilen – geht das?

Policy Brief #1
des Digital Autonomy Hubs
Dezember 2020

Autorin:
Friederike Reinhold
Senior Policy Advisor, AlgorithmWatch

Korrektorat:
Karola Klatt

Layout:
Beate Autering

Veröffentlicht von

AW AlgorithmWatch gGmbH
Linienstr. 13
10178 Berlin

Gesellschaft für Informatik e.V. (GI)
Spreepalais am Dom
Anna-Louisa-Karsch-Straße 2
10178 Berlin

Kontakt:
info@digitalautonomy.net

Der Digital Autonomy Hub wird gefördert vom

Bundesministerium für Bildung und Forschung

im Rahmen des Forschungsprogramms „Technik zum Menschen bringen"