ABIDA – Assessing Big Data
Expertenworkshop Vertiefungsstudie Heim und Freizeit
Kassel 28.06.2018

Digitale Souveränität in Zeiten ubiquitärer Datenverarbeitung?

Eine vergleichende exemplarische Diskussion der Möglichkeiten und Grenzen technischer und nicht-technischer Lösungsansätze zur Gewährleistung der informationellen Selbstbestimmung am Beispiel von Big Data im Bereich Heim und Freizeit

Ergebnisprotokoll

Im Rahmen des ABIDA-Projekts fand am 28. Juni 2018 in Kassel der ABIDA-Expertenworkshop zur Vertiefungsstudie Heim und Freizeit statt. Ziel des Workshops war es, Möglichkeiten und Grenzen technischer und nicht-technischer Lösungsansätze zur Gewährleistung der informationellen Selbstbestimmung in Zeiten von Big Data zu diskutieren und Handlungsoptionen für Politik, Forschung und Entwicklung zu entwerfen. Im Rahmen des Workshops wurden dazu die zentralen Thesen der beiden ABIDA-Gutachten „Big Data im Bereich Heim und Freizeit mit Fokus Smart Living“ (ConPolicy / Stiftung Neue Verantwortung) und „Datenrechte: – eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland-USA (Prof. Louisa Specht / Prof. Wolfgang Kerber) diskutiert. Das Programm des Workshops orientierte sich an den wesentlichen Eckpunkten des Koalitionsvertrags zur zukünftigen Digitalpolitik (Förderung eines innovativen Einwilligungsmanagements S. 47; Klärung der Sinnhaftigkeit von Dateneigentum S. 129). Zentrale Forderungen des Sachverständigen Rates für Verbraucherfragen zu verbraucherzentrierten Dashboards, Datentresoren und persönlichen Datenclouds wurden zudem einer kritischen Analyse unterzogen.

Ergebnisse Slot 1: Dateneigentum – ein Weg zu mehr Transparenz und Kontrolle?

Mit einem Impulsvortrag von Prof. Wolfgang Kerber zu den Kernthesen des Gutachtens Specht/Kerber „Datenrechte – eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland-USA“

Die schon länger währende wissenschaftliche und politische Diskussion um das Dateneigentum wird insgesamt als wenig zielführend erachtet. Vor allem einer metaphorischen Redeweise, die suggeriert, der Endverbraucher würde mit Dateneigentum informierter einwilligen und mehr Kontrolle über seine Daten haben, da er sie nun sprichwörtlich „besitzt“, gilt es entschieden entgegenzutreten. Dateneigentum ist nicht per se ein Instrument für mehr Kontrolle, Sicherheit und Transparenz. Verschiedene technische als auch

nicht-technische Maßnahmen zur Erhöhung der Transparenz und Informiertheit der Verbraucher bzw. zur Verbesserung der Betroffenenrechtedurchsetzung bedürfen stattdessen der separaten Diskussion – wie in den beiden weiteren Slots des Workshops vorgesehen.

Es kann festgestellt werden: Dateneigentum als Ausschließlichkeitsrecht mit Nutzungs- und Ausschlussfunktion ist für eine vertragliche Nutzung von Daten auf dem Sekundärmarkt nicht erforderlich. Das bestehende Instrumentarium aus Kaufrecht, Werkvertragsrecht, Pachtvertragsrecht bzw. des wettbewerbsrechtlichen Investitionsschutzes erscheint ausreichend. Eine ökonomische Notwendigkeit zur Schaffung eines Dateneigentums/Datenerzeugerrechts ist zudem nicht erkennbar. Innovationsanreize zur Datenproduktion sind nicht notwendig. Exklusive Eigentumsrechte an Daten können Innovationen in digitalen Ökonomien sogar behindern.

Eine eigentumsrechtliche Ausgestaltung von personenbezogenen Daten auf dem Primärmarkt ist aufgrund des Persönlichkeitsrechts allenfalls als Lizenz möglich, was jedoch keine klar erkennbaren Vorteile gegenüber einer schuldrechtlichen Ausgestaltung hätte (sofern eine schuldrechtliche Ausgestaltung als notwendig erachtet wird, siehe hierzu die Ausführungen unten zu Datenschuldrecht).

Die Diskussionen um das Dateneigentum sollten insgesamt auf sekundärmarktlicher Seite einer Diskussion um Zugangsrechte weichen, wobei Interessenkonflikte umfassend durchdacht und regulierende Eingriffe in den Markt ex ante untersucht werden sollten. Lösungen sind dabei branchen- und kontextspezifisch zu erarbeiten, was am Beispiel der unterschiedlichen Akteure im Bereich Connected Car auf dem Workshop ausführlich diskutiert wurde. Unter bestimmten Bedingungen können Zugangsrechte gerechtfertigt sein, aber die genaue Ausgestaltung erfordert sorgfältige Analyse und kann in verschiedenen Kontexten sehr unterschiedlich ausfallen. Marktliche Regulationserfordernisse sind anhand empirischer Fakten zu benennen und hinsichtlich ihrer Erforderlichkeit und Angemessenheit situational genau zu begründen.

Unklar blieb auch nach längerer Diskussion, inwiefern auf primärmarktlicher Seite die Etablierung eines sog. Datenschuldrechts erforderlich und auch ökonomisch notwendig ist, um diejenigen Geschäftsmodelle (besser?) abzustützen, die Daten als Entgelt behandeln. Die Diskussionen um das Datenschuldrecht werden insofern zusätzlich dadurch erschwert, als dass noch erhebliche Unsicherheiten darüber bestehen, wie absolut das Kopplungsverbot auszulegen ist (Art. 7 Abs. 4 DS-GVO) bzw. welchen Stellenwert „berechtigte Interessen“ Art. 6 Abs. 1 lit. f DS-GVO und „vertragliche Erforderlichkeit“ Art. 6 Abs. 1 lit. b DS-GVO (neben der „Einwilligung“ Art. 6 Abs. 1 lit. a DS-GVO) als Rechtsgrundlage für die Datenverarbeitung in datengetriebene Geschäftsmodelle haben können.

Einigkeit herrscht insgesamt darüber, dass eine mögliche zivilrechtliche Anerkennung der datenschutzrechtlichen Einwilligung als „geschuldete Gegenleistung eines zivilrechtlichen Vertrags“ nicht zu einem weniger an Datenschutz bei den Betroffenen führen darf (etwa indem der Widerrufbarkeit der Einwilligung eingeschränkt oder gänzlich aufgehoben wird). Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil

von 1983 die informationelle Selbstbestimmung auch in den Zusammenhang mit der Menschenwürde gestellt, was eine unmittelbare Beschränkung der Widerrufbarkeit ausschließt.

Insgesamt wurden auch die Möglichkeiten eines Datenschuldrechts auf europäischer Ebene problematisiert: Die vorgeschlagene Anwendung des Abstraktions- und Trennungsprinzip auf das Datenschuldrecht erweist sich als eine bundesdeutsche Spezifität. Das französische, belgische, luxemburgische, italienische, spanische und portugiesische Zivilrecht kennt keine Unterscheidung zwischen Kausal- und Verfügungsgeschäft (und damit verbunden: einem Trennungs- und Abstraktionsprinzip). Die Notwendigkeit als auch die Konturen eines Datenschuldrechts bedürfen evtl. der weiteren Forschung – auch hinsichtlich der Effekte auf den europäischen Binnenmarkt (falls nationale Lösungen des Vertragsrechts in Konkurrenz zueinander treten sollten).

Ergebnisse Slot 2: Datenportabilität, Dashboards, Datentresore, persönliche Datenclouds, Sticky Policies – Effektive Mittel der informationellen Selbstbestimmung oder trojanisches Pferd einer Ökonomisierung?

Mit Impulsvorträgen von Frederick Richter LL.M. „Das neue Recht auf Datenübertragbarkeit" und Dr. Nicola Jentzsch „Marktdynamiken der persönlichen Datenökonomie"

Mit Art. 20 DS-GVO statuiert der Gesetzgeber ein Recht auf Datenübertragbarkeit für den Endverbraucher: Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten bzw. diese an einen anderen Verantwortlichen übertragen zu lassen. Durch die Datenübertragung dürfen aber keine Rechte und Freiheiten Dritter beeinträchtigt werden (was z. B. der Fall sein könnte, wenn Facebook-Kommunikationsdaten zu einem anderen Anbieter mitgenommen werden sollen). Das ursprüngliche Ziel, mit dem Recht auf Datenportabilität den Wettbewerb anzuregen, gerät damit in Gefahr.

Das Recht auf Datenportabilität garantiert insgesamt keine Datenkompatibilität bzw. nahtlose Interoperabilität. Marktliche Standards, die es ermöglichen, portierte Daten von einem DV-System eines Anbieters in das DV-System eines anderen Anbieters zu überführen, gibt es bisher nicht. Die Industrie zeigt sich hier auch nicht sonderlich eigeninitiativ. JSON und XML sind mögliche Formate der Datenübertragung. Deren Semantik ist jedoch nicht standarisiert. Zu kaum lösbaren Inkompatibilitäten kann es vor allem dann kommen, wenn inkommensurable Semantiken vorliegen und ein Anbieter z. B. zur Bewertung ein 4-Sterne-System verwendet, der andere Anbieter ein 5-Sterne-System. Eine genauere Bestimmung der Datenkategorien, die unter das Recht der Datenportabilität fallen, tut not.

Das Ausüben des Rechts auf Datenportabilität ist insgesamt nicht gleichzusetzten mit der Löschung von Daten bzw. der Kündigung vertraglicher Verhältnisse. Beide bleiben nach einer Portierung beim ursprünglichen Anbieter bestehen. Im Sinne der Datensparsamkeit ist dies kritisch zu bewerten, denn mit der Datenübertragung geht eine Vervielfältigung des Datensatzes einher. Dies führt insgesamt zur Forderung, dass Betroffene transparent darauf hingewiesen werden sollten, dass mit der Datenübertragung an eine andere

Stelle weder eine automatische Löschung beim alten Anbieter noch eine Kündigung bestehender Verträge einhergeht.

Doch nicht nur der Grundsatz der Datenminimierung erfährt durch die Datenportabilität eine Relativierung, sondern auch der Grundsatz der Zweckbindung (und damit die kontextuelle Integrität der Datenverarbeitung). Betroffene Personen könnten von Datensammlern bzw. Unternehmen animiert werden, ihre Daten für weiterführende Big-Data-Analysen entgeltlich/unentgeltlich gemäß Artikel 20 DS-GVO übertragen zu lassen bzw. in einem maschinenlesbaren Format zur Verfügung zu stellen (etwa für Zwecke des Scorings o. ä.). Werden Profiling / Scoring und individuell-risikobasierte Verträge zum Standard, können auch Marktdynamiken entstehen, in der der Verbraucher unter Druck gerät, seine Daten preisgeben zu müssen (wodurch der Aspekt der Freiwilligkeit der Einwilligung in die Datenverarbeitung ebenfalls relativiert wird). In der wirtschaftswissenschaftlichen Forschung ist dieses Phänomen als Unraveling-Gleichgewicht bekannt, also ein Gleichgewicht, in dem die Privatsphäre erodiert beziehungsweise sich auflöst. Eine individuelle Bepreisung und Scoring-basierte Tarifierung führt insgesamt zu einer Umverteilung der ökonomischen Renten in der Bevölkerung und evtl. neuen Formen der Diskriminierung. Eine Beforschung der gesellschaftlichen Effekte ist deshalb frühzeitig angezeigt.

Das Recht auf Datenübertragbarkeit kann insgesamt auch (gewollt?/ungewollt?) eine persönliche Datenökonomie befördern, indem Nutzerinnen und Nutzer ihre heruntergeladenen Daten gewinnbringend an unterschiedliche Akteure verkaufen – mit unklaren Vorteilen und Nachteilen für den Verbraucher. Ein in der Praxis funktionierendes Recht auf Datenportabilität bildet dann die Grundlage sog. persönlicher Datenclouds, Datentresore bzw. Personal-Information-Management-Systems (PIMS). Die Chancen und Risiken derartiger Systeme sind aus verhaltenspsychologischer und verhaltensökonomischer Perspektive jedoch noch eingehender zu untersuchen, insbesondere wie informiert in Zweckänderungen / Kontext-Switches der Datenverarbeitung eingewilligt werden kann bzw. inwieweit hier auch Schutzpflichten von Seiten des Staates tangiert sind. Von einem funktionierenden Markt von Personal-Information-Management-Systemen kann insgesamt nicht gesprochen werden, auch weil das dafür erforderliche Recht auf Datenportabilität in der Praxis nur unzureichend umgesetzt ist.

Von Personal-Information-Management-Systemen sind sog. Dashboards zu trennen, die als Webfrontend reine Instrumente der Durchsetzung von Betroffenenrechte sind (wie das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung / Widerruf etc.). Die entsprechende Internetseite bietet nach Authentifizierung und Autorisierung die Möglichkeit zur Kommunikation mit dem Verantwortlichen der Datenverarbeitung bzw. der einfachen Ausübung von Betroffenenrechte (im Sinne eines Self-Service-Centers). Dashboards – manchmal auch als verbraucherzentrierte Datenportale bezeichnet – würden sich auch gerade für die Ausübung des Rechts auf Datenportabilität anbieten. Dashboards, die über Schnittstellen unterschiedliche Dashboard-Webservices verschiedener Anbieter ansprechen können und dem Nutzer eine zentralisierte Datenkontrolle in Form eines One-Stop-Shop-Verfahren ermöglichen, firmieren ebenfalls oft unter dem Titel Personal-Information-Management-System oder schlicht Dashboard.

Die Wirksamkeit von Art. 20 DS-GVO sollte insgesamt einem Praxistest unterzogen werden (u. a. mit verhaltensökonomischen Untersuchungen zur Bereitschaft der Verbraucher, die Portabilitätsmöglichkeiten auch tatsächlich zu nutzen und zu welchem Zweck). Der ursprüngliche Normzweck (Wettbewerbsstärkung) ist mit der Rechtswirklichkeit und evtl. weiteren, nicht primär intendierten(?) Zwecken (persönliche Datenökonomie) abzugleichen. Die Ergebnisse sollten in die regelmäßigen Evaluierungszyklen der DS-GVO einfließen.

Mit der „Data Privacy Vocabluaries and Controls Group" ist das W3-Konsortium bestrebt, einen Standard für „Sticky Policies" und die elektronische Wahrnehmung von Betroffenenrechte zu etablieren, der auf die wesentlichen strukturellen Neuerungen der DS-GVO reagiert. Die Idee, Verarbeitungsrechte als Metadaten zusammen mit den Daten abzulegen bzw. diese kryptographisch miteinander zu verbinden, ist dabei nicht neu. Das Konzept weist damit gewisse Parallelen zum Digitial-Rights-Management aus dem Bereich Film/Musik auf mit dem Unterschied, dass die Ende-zu-Ende-Verschlüsselung nicht im Analogen endet, sondern im Digitalen verbleibt. Das Konzept bietet damit keinen absoluten Schutz gegen zweckändernde Verarbeitung und unerlaubtes Kopieren und Nutzen. Es ist getragen von der Annahme, dass der Datenverarbeiter einen Willen zum rechtskonformen Handeln und Compliance besitzt. Derartige Systeme können somit z. B. effektiv bei der Einhaltung von Löschfristen unterstützen. Auf eine kryptographische Bindung wird insgesamt verzichtet, weil dies eine performante Big-Data / Linked-Data-Analyse zusätzlich erschweren würde.

Ergebnisse Slot 3: Aktuelle technische und nicht-technische Ansätze zur Gewährleistung digitaler Souveränität in Zeiten von Big Data: Quadratur des Kreises?

Mit Impulsvorträgen von Dr. Sara Elisa Kettner „Von One-Pagern und Privacy-Bots. Neuere Wege der informierten Einwilligung" und Harald Zwingelberg „Neue Wege bei der Einwilligung: Technische und nicht-technische Ansätze im Zeitalter von Big Data"

Die Rahmen des ABIDA-Gutachtens „Heim und Freizeit" wurden exemplarisch 22 Smart-Home-Anwendungen aus den Bereichen smarte Beleuchtung, vernetze smarte Videokameras und Sprachassistenzsysteme untersucht. Es wurde dabei deutlich, dass einige Produkte über gar keine Datenschutzerklärung verfügten, obwohl dies rechtlich erforderlich ist. Datenschutzerklärungen waren z. T. auch nur in englischer Sprache abgefasst, was eine Hürde für Verbraucher darstellt, die der englischen Sprache nicht mächtig sind. Viele der Datenschutzerklärungen waren insgesamt sehr lang. Bei den untersuchten Sprachassistenz-Systemen betrug die Lesedauer im Schnitt ca. 15 Minuten. Vom Sprachniveau waren die Datenschutzerklärungen vorwiegend in komplexer Fachsprache abgefasst, was in einen gewissen Widerspruch zur Forderung von Art. 12 Abs. 1 DS-GVO tritt, die Datenschutzerklärung in „klarer und einfacher Sprache" abzufassen.

Weitere Untersuchungen von ConPolicy im Rahmen der Einwilligung in die Datenverarbeitung beim Online-Shopping zeigen zudem sehr geringe Leseraten von Datenschutzerklärungen: Nur 0.2% der Online-Shopper haben vor Vertragsschluss den Link zur Datenschutzerklärung angeklickt.

Mittels verschiedener technischer Maßnahmen kann die Lektüre der Datenschutzerklärung zwar zu einem gewissen Maße erzwungen werden, indem 1) der Kauf nur abgeschlossen werden kann, wenn der Link zur Datenschutzerklärung angeklickt wurde, 2) die Schaltfläche „Akzeptieren" unter die Datenschutzerklärungen gesetzt wird sodass diese nur durch Scrollen durch die Datenschutzerklärung erreicht werden kann bzw. 3) die Schaltfläche „Akzeptieren" für eine gewisse Zeit „deaktiviert" ist, um das zu schnelle Wegklicken der Datenschutzerklärung zu vermeiden. Der Nutzen für Betroffene ist jedoch noch nicht wissenschaftlich untersucht und so bleibt die Wirksamkeit der Maßnahmen bezüglich ihrer Informiertheit unklar.

In letzter Zeit werden deshalb „Datenschutzerklärungen auf einer Seite", sog. One-Pager, vermehrt diskutiert, die die Informiertheit der Verbraucher nachhaltig erhöhen sollen (wobei Art. 12 Abs. 7 DS-GVO ausdrücklich dazu ermuntert, Bildsymbole für überblicksartige Darstellungen zu verwenden). Neuere verhaltenspsychologische Untersuchungen zeigen zwar, dass One-Pager in der Tat öfter gelesen werden als normale Langfassungen, die Informiertheit / das Verständnis über die Datenverarbeitungsvorgänge jedoch insgesamt nicht signifikant erhöht ist. One-Pager können deshalb nur als ein Baustein betrachtet werden neben anderen wie a) Drill-Down-Funktionalitäten / Layered-Approaches, b) standardisierte Bildsymbole / Piktogramme / Warnhinweise, c) tabellarischen Zusammenfassungen etc.

Eine Art von Datenbrief / One-Pager kann auch auf der Verpackung von smarten Produkten und „Internet of Things"-Geräten angebracht werden. Er informiert über die wesentlichen Eckpunkte der Datenverarbeitung. Über einen aufgedruckten QR-Code kann dann die Langfassung mittels Smartphone aufgerufen werden. Die Forderungen weisen damit gewisse Parallelen zu anderen Diskussionen auf, etwa um den „Datenausweis" beim Connected Car (der in Form eines Informationsblatts über die Datenverarbeitung bzw. die Informationsflüsse vom Auto / zum Auto informieren soll).

Vielversprechend bzgl. Transparenzerhöhung erscheinen insgesamt die neuen Ansätze der Privacy-Bots bspw. in Form des BMBF-geförderten DATENSCHUTZscanners: Derartige Softwaresysteme untersuchen / parsen Datenschutztexte, verdichten Informationen entsprechend der Präferenzen der Nutzer und lenken die Aufmerksamkeit selektiv auf spezifische Aspekte, die als besonders relevant erachtet werden. Nach der technischen Entwicklung von Prototypen steht eine Evaluierung hinsichtlich der praktischen Handhabbarkeit für den Nutzer noch aus. Auch wurde der Aspekt der verbesserten Informiertheit noch nicht untersucht.

Die Untersuchung von Dashboards/Datenportalen auf das Verhalten von Verbrauchern und deren Informiertheit steht ebenfalls noch aus. Immerhin halten 87% der Verbraucher in einer Umfrage den Zugang zu einem Datenportal für wichtig. 92% befürworten eine Löschfunktion in den Dashboards.

Eine Standardisierung von Piktogrammen / Bildsymbolen bzw. Vorgaben zur einheitlichen Abfassung von Datenschutzerklärungen könnten insgesamt hilfreich sein. Es wurden aber auch die Grenzen deutlich: Fehlendes Hintergrundwissen über Datenschutz erlaubt es vielen Personen oft nicht, die Bildsymbole überhaupt zu verstehen (was noch einmal nachdrücklich die Notwendigkeit einer angemessenen Bildung für eine digitale Welt betont). Die Visualisierung datenschutzrechtlicher Aspekte („sensitive Kategorien", „Weiterleitung an Dritte" etc.) erweist sich als schwierig.

Der Aspekt der Vergleichbarkeit von Datenschutzerklärungen in Form von One-Pagern wurde andiskutiert, indem Parallelen zu Energieeffizienz-Labeln von Elektrogeräten gezogen wurden. Derartige Labels erlauben das einfache Vergleichen von Produkten. Es bedarf der weiteren Forschung, inwiefern die tatsächliche Komplexität der Datenverarbeitung, die Verschiedenartigkeit der Datenverarbeitung unterschiedlicher Anbieter gleicher Produkte in wenigen Symbolen / Faktoren verdichtet werden kann bzw. inwiefern Quantifizierungen / Ampeln etc., die Vergleiche ermöglichen sollen, nur eine Schein-Exaktheit einführen (und damit neue Gefahren und Intransparenzen induzieren würde).

Die erforderlichen Anstrengungen auf Seiten des Nutzers bzgl. einer informierten Einwilligung und einer nur schwierig zu bewältigenden Analyse der komplexen Datenverarbeitungsvorgänge steht einem gewissen Bequemlichkeitsdenken entgegen, weshalb sich gewisse Forschungslinien auch mit automatisierten Einwilligungsassistenten beschäftigen, die formalisierte und maschinenlesbare Datenschutzerklärungen / Policies mit den Nutzerpräferenzen abgleichen und den Verbraucher so komplett von der Einwilligung entlasten. Nicht nur aus rechtlicher Perspektive ist zu prüfen, inwiefern derartige Systeme überhaupt einsetzbar wären, fordert doch Art. 4 Nr. 11 DS-GVO eine „eindeutig bestätigende Handlung" Seiten des Nutzers. Auch ist aus informatischer Perspektive nach der Zuverlässigkeit dieser im Hintergrund agierender Systeme zu fragen, die selbst wiederum neue Intransparenzen schaffen und neue Fragen der Haftung aufwerfen. Oder um es in den Worten der Metapher des Internetführerscheins zu sagen: Wie können wir sicherstellen, dass uns derartig automatisierte Systeme auf der Datenautobahn nicht an die Wand fahren? Die Diskussionen um die Zuverlässigkeit Künstlicher Intelligenz und den Grenzen von Deep Learning haben mit den jüngsten Unfällen beim automatisierten Fahren erst begonnen.

Teilnehmerinnen und Teilnehmer

Andreas Czech (ABIDA-Team, Karlsruher Institut für Technologie KIT)

Thilo Goeble (in Vertretung Prof. Hornung, Universität Kassel)

Dr. Nicola Jentzsch (Stiftung Neue Verantwortung)

Prof. Dr. Wolfgang Kerber (Philipps-Universität Marburg)

Dr. Sara Elisa Kettner (ConPolicy GmbH – Institut für Verbraucherpolitik)

Daniel Möller (Philipps-Universität Marburg)

David Nink (in Vertretung Prof. Martini, Universität Speyer)

PD Dr. Oliver Raabe (Karlsruher Institut für Technologie KIT)

LL.M. Frederick Richter (Vorstand Stiftung Datenschutz)

Dr. Oliver Siemoneit (ABIDA-Team, Karlsruher Institut für Technologie KIT)

Tristan Tillmann (ABIDA-Team, Universität Münster)

Dr. Thilo Weichert (Netzwerk Datenschutzexpertise)

Harald Zwingelberg (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)

Begleitforschung Big Data „ABIDA – Assessing Big Data“

Gefördert vom Bundesministerium für Bildung und Forschung BMBF

(Förderkennzeichen 01IS15016A-F)

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung