NEUE DATENINTERMEDIÄRE

Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder

15. September 2020

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. DIE KERNPOSITIONEN IM ÜBERBLICK

- Es bedarf eines gesetzlichen Rahmens, der sicherstellt, dass neue Datenintermediäre, wie „Datentreuhänder“ oder „Personal Information Management Systems” (PIMS), unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse an der Verwertung der im Auftrag der Verbraucherinnen und Verbraucher[1] verwalteten Daten agieren und somit Interessenkonflikte ausgeschlossen werden können.
- In diesem Rahmen müssen Treuepflichten der Datenintermediäre gegenüber den Nutzern präzise gefasst werden. Es sollten Regelungen zur Zulässigkeit und Grenzen rechtsgeschäftlicher Mandate formuliert sowie hohe Anforderungen an die Transparenz und Angemessenheit von Geschäftsbedingungen gestellt werden. Eine potentielle Monopolstellung muss verhindert und Koppelungen unterbunden werden. Weiterhin sollten Vorkehrungen für den Fall der Insolvenz oder Auflösung definiert werden.
- Qualitätsanforderungen sollten gesetzlich festgeschrieben werden. Es bedarf strikter Vorgaben hinsichtlich der Datensicherheit, insbesondere der Qualität der Verschlüsselung der Daten sowie der Datenübertragungen, aber auch hinsichtlich angemessener Anonymisierungsverfahren. Vor Inbetriebnahme sollten Datenintermediäre zwingend eine Datenschutz-Folgenabschätzung durchführen sowie die zuständigen Datenschutzaufsichtsbehörden konsultieren müssen. Außerdem sollte eine Zertifizierung mit einer entsprechenden Überwachung obligatorisch sein.
- Es bedarf einer Auseinandersetzung mit der Frage, inwieweit Datenintermediäre die Datennehmer überprüfen und deren Zuverlässigkeit gewährleisten sollten. Wichtig wäre weiterhin, dass Haftungsfragen geregelt werden.
- Es sollte eine umfassende Kooperation aller Verantwortlichen mit den Datenintermediären sichergestellt werden. Darüber hinaus sollte der Austausch über und die Entwicklung von Interoperabilitäts- und Portabilitätsstandards sowie offenen Schnittstellen gefördert werden.

[1] Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

II. EINLEITUNG

Im Februar 2020 veröffentlichte der Verbraucherzentrale Bundesverband (vzbv) das Positionspapier „Personal Information Management Systems (PIMS) – Chancen, Risiken und Anforderungen“, um einen konstruktiven Beitrag zur beginnenden öffentlichen Diskussion beizutragen, die sich rund um das Schlagwort „Datentreuhänder“ gebildet hatte. In den vergangenen Monaten hat die Debatte an Fahrt aufgenommen. Weitere Organisationen veröffentlichten Papiere zu diesem Themenkomplex und in einer Vielzahl von Veranstaltungen wurde das Thema intensiv diskutiert. Inzwischen wurden auch legislative Maßnahmen auf nationaler[2] und europäischer Ebene[3] angekündigt.

Weiterhin ist die Debatte jedoch von einer gewissen Diffusität geprägt. Noch immer sind weder die Begrifflichkeiten der Datentreuhänder sowie der PIMS klar umrissen, noch gibt es ein einheitliches Verständnis über die Rollen und Zielsetzungen dieser – wie sie inzwischen meist bezeichnet werden – „neuen Datenintermediäre“. Verkürzt lässt sich sagen, dass Datentreuhändern eher die Rolle eines Datenverwalters zugedacht wird, das wesentliche Merkmal der PIMS hingegen das Einwilligungsmanagement ist. Sprich: Verbraucherinnen und Verbraucher sollen an einer zentralen Stelle festlegen können, wie, für welche Zwecke und durch welche Stellen ihre Daten verarbeitet werden dürfen.

Im Laufe der Diskussion hat sich jedoch auch gezeigt, dass der bisher starke Fokus des vzbv auf PIMS zu kurz gegriffen war, da eine klare Abgrenzung zu anderen Datenintermediären weder möglich noch zielführend ist. Gemein haben alle Ansätze (soweit personenbezogene oder anonymisierte Daten verarbeitet werden), dass mit ihnen die Hoffnung verbunden wird, die Verarbeitung beziehungsweise den Austausch von Daten zu erleichtern, ohne dabei Abstriche beim Schutz der personenbezogenen Daten der Betroffenen machen zu müssen. Gleichermaßen besteht bei allen Ansätzen die erhebliche Gefahr, dass die Grundrechte und Grundfreiheiten der betroffenen Personen verletzt werden können. Aufgrund der großen Gemeinsamkeiten lassen sich die vom vzbv bisher genannten Anforderungen an PIMS auch weitgehend auf andere Datenintermediäre übertragen.

Nach Ansicht des vzbv bedarf es insbesondere eines gesetzlichen Rahmens, der die Zulässigkeit und Grenzen der Datenintermediäre regelt, Treuepflichten normiert, konfligierende Interessen ausschließt sowie entsprechende Kontroll- und Sanktionsmöglichkeiten schafft. Innerhalb dieses Rahmens könnten sich dann die verschiedenen Modelle weiterentwickeln und zu einem echten gesamtgesellschaftlichen Mehrwert führen. Nach Einschätzung des vzbv bestehen jedoch durch die staken Bezüge zum Datenschutz und den Vorrang der Datenschutz-Grundverordnung (DSGVO) auf nationaler Ebene nur höchst eingeschränkte Möglichkeiten einer entsprechenden Regulierung.

---

[2] Dachwitz, Ingo; et. al.; Netzpolitk.org: Lebensverlängernde Maßnahmen für ein kaputtes Geschäftsmodell (2020), URL: https://netzpolitik.org/2020/online-tracking-lebensverlaengernde-massnahmen-fuer-ein-kaputtes-geschaeftsmodell/ [Zugriff: 18.08.2020].

[3] European Commission: Inception impact assessment - Ares(2020)3480073 (2020), URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces [Zugriff: 18.08.2020].

III. WAS SIND „DATENTREUHÄNDER“?

Der Begriff des „Datentreuhänders“ umfasst eine Vielzahl von verschiedenen Konzepten, die jedoch völlig unterschiedliche Konstruktionen aufweisen und verschiedenste Zielrichtungen verfolgen können.[4][5] In erster Linie sollen sie jedoch die Rolle eines neutralen Datenverwalters einnehmen. Zwei Beispiele:

Eine Form von Datentreuhändern ist bereits seit vielen Jahren im Datenschutzrecht ein etabliertes Konzept zur Pseudonymisierung von Daten. „Im klassischen Treuhändermodell ist der Treuhänder eine juristische Person außerhalb des Verantwortlichen oder Auftragsverarbeiters, mithin ein ‚Dritter‘. Er ist somit eine von der Datenerhebung und Datenauswertung räumlich und organisatorisch unabhängige Vertrauensstelle. Ein Treuhänder kann beispielsweise mit der Aufbewahrung von Schlüsseln zur Re-Identifizierung von Betroffenen betraut werden“.[6] Dies bedeutet also beispielsweise, dass zwischen einem Unternehmen, das über Rohdaten verfügt und einem Unternehmen, das auf dieser Basis Big-Data-Analysen durchführen soll, ein „Datentreuhänder“ beauftragt wird, der die Daten pseudonymisiert und nur in dieser pseudonymen Form zu Analysezwecken weitergibt. Der Treuhänder löscht anschließend die Daten, so dass er – und nur er – noch über den Pseudonymisierungsschlüssel verfügt. Dieses Modell wird unter anderem im Bereich der medizinischen Forschung und der Biobanken erfolgreich eingesetzt.

Ein weiteres Beispiel für einen Datentreuhänder liefert die Debatte um die rechtssichere Gestaltung des automatisierten Fahrens. Um mögliche Unfälle aufklären zu können, ist es notwendig aufzuzeichnen, ob automatisierte Fahrfunktionen oder der Fahrzeugführer das Kraftfahrzeug gesteuert haben und ob technische Störungen vorlagen. Eine Speicherung der Daten allein in den Fahrzeugen oder im Backend der Hersteller ist für diesen Zweck nicht zielführend, weil diese in streitigen Fragen darüber, ob Mensch oder System gefahren ist, Partei sind und insoweit ein Zugriff der Hersteller auf die Fahrmodusdaten ausgeschlossen sein muss. Daher hat sich der vzbv für die Speicherung dieser Fahrmodusdaten im Kraftfahrzeug und zur Absicherung bei einer staatlichen oder beliehenen Stelle auf Basis einer gesetzlichen Grundlage ausgesprochen.[7][8]

---

[4] Vgl. auch Blankertz; Aline: Designing Data Trusts (2020), URL: https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_d.pdf [Zugriff: 24.08.2020].

[5] Vgl. Rat für Informationsinfrastrukturen: Datentreuhandstellen gestalten (2020), URL: http://www.rfii.de/?wpdmdl=4259 [Zugriff: 18.08.2020].

[6] Fokusgruppe Datenschutz des Digital-Gipfels: Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung (2019), S. 16, URL: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf?__blob=publicationFile&v=2 [Zugriff: 10.02.2020].

[7] Vgl. Verbraucherzentrale Bundesverband: Rechtssicher fahren mit automatisierten Fahrzeugen (2017), S. 14, URL: https://www.vzbv.de/sites/default/files/downloads/2017/03/21/2016-12-30_stn_zum_gesetzentwurf_aend_stvg_neu.pdf [Zugriff: 10.02.2019].

[8] Vgl. Gemeinsamer Brief des ADAC, VdTÜV, GDV und vzbv an Bundesminister Andreas Scheuer zum Speicherort des Fahrmodusspeichers nach § 63a StVG vom 16.07.2019.

IV. WAS SIND „PIMS“?

PIMS haben einen anderen Fokus als die oben genannten Datentreuhänder. Hintergrund ist insbesondere die seit einigen Jahren schwelende Kritik an der datenschutzrechtlichen Einwilligung. Demnach sei es bei den heute dominierenden Massengeschäften und der Komplexität der Technologie und der Geschäftsmodelle für die Betroffenen nahezu unmöglich, tatsächlich informierte Einwilligungen in die Verarbeitung ihrer personenbezogenen Daten zu treffen. Außerdem sei es für die Betroffenen schwierig nachzuvollziehen, welchen Unternehmen gegenüber in der Vergangenheit eine Einwilligung abgegeben wurde, um diese gegebenenfalls wieder zurückzuziehen. An dieser Stelle sollen die PIMS ansetzen, indem sie den Betroffenen in erster Linie das Einwilligungsmanagement erleichtern.

> Bei PIMS handelt es sich „um neue Technologien und Ökosysteme, mit denen Menschen in die Lage versetzt werden sollen, über die Erhebung und Weitergabe ihrer personenbezogenen Daten Kontrolle auszuüben.“[9] Kerngedanke dieses Konzeptes ist, den einzelnen Verbraucher in das Zentrum des Datenmanagements zu stellen.[10]

Bereits im September 2016 veröffentlichte der Europäische Datenschutzbeauftragte eine entsprechende Stellungnahme, in der der Frage nachgegangen wurde, wie PIMS zu einem besseren Schutz personenbezogener Daten beitragen können und welche Herausforderungen dabei bestehen.[11] Auch die EU-Kommission veröffentlichte im November 2016 einen Bericht, in der sie sich mit den Chancen und Risiken von PIMS auseinandersetzte.[12] Und jüngst stellte die Datenethikkommission der deutschen Bundesregierung (DEK) die Vorteile und Risiken von PIMS heraus.[13]

Derzeit gibt es eine Vielzahl von verschiedenen PIMS-Konzepten[14], die sich in ihrer Zielsetzung, Geschäftsmodellen, Reichweite (z.B. branchenbezogen oder universell) sowie ihrer technischen und organisatorischen Ausgestaltung stark unterscheiden.[15] Gleichzeitig sind viele der Konzepte noch nicht sehr ausgereift. Somit unterscheiden sich auch die Art der potentiellen Chancen und die Größe der Risiken erheblich.

---

[9] Europäischer Datenschutzbeauftragter: Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM). Stellungnahme 9/2016 (2016), S. 6, URL: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf [Zugriff: 10.02.2020].

[10] Dies ist bei den zuvor angeführten Konzepten nicht der Fall.

[11] Europäischer Datenschutzbeauftragter (EDSB) (2016) (wie Anm. 8).

[12] European Commission: An emerging offer of "personal information management services" (2016), URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 [Zugriff: 10.02.2020].

[13] Datenethikkommission der Bundesregierung (2019) (wie Anm. 3), S. 133ff.

[14] Vgl. Stiftung Datenschutz: Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Studie (2017), S. 20ff, URL: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf [Zugriff: 10.02.2020].

[15] Unterscheidungen können beispielsweise sein: Werden die Daten lokal beim Betroffenen gespeichert oder in der Cloud? Wenn auf Daten aus verschiedenen Quellen zugegriffen werden soll, werden diese im PIMS gespeichert oder verbleiben die Daten bei den ursprünglichen Quellen und der PIMS stellt lediglich eine Art Verlinkung her? Haben potentielle Datennutzer direkten Zugriff auf die Daten oder erfolgt die Analyse auf den PIMS (die dann Beschränkungen vorgeben könnten) oder erfolgt die Analyse durch die PIMS und es werden lediglich Ergebnisse übermittelt?

V. ANFORDERUNGEN AN „NEUE DATENINTERMEDIÄRE“

Auch wenn die neuen Datenintermediäre die digitale Selbstbestimmung des Einzelnen fördern sollen, können von ihnen Gefahren ausgehen. So sieht beispielsweise die DEK das Risiko, dass Verbraucher auf einen Weg der unbewussten oder sorglosen Fremdbestimmung geführt werden könnten. Insbesondere würde es der Idee der Datenintermediäre widersprechen, wenn Entscheidungen in wesentlichem Umfang von Betroffenen an die Betreiber abgegeben oder Entscheidungen Betroffener durch diese interessenwidrig beeinflusst werden.[16]

Um den Gefahren der Datenintermediäre zu begegnen, sollte ein – zum Teil über die DSGVO hinausgehender, zum Teil die DSGVO präzisierender – rechtssicherer Rahmen auf europäischer Ebene geschaffen werden. Nur mit einem solchen Rahmen wird das Ziel erreicht werden können, mit Hilfe dieser Datenintermediäre die Verarbeitung beziehungsweise den Austausch von Daten zu erleichtern, ohne dabei Abstriche beim Schutz der personenbezogenen Daten der Betroffenen machen zu müssen.

Durch einen solchen Rahmen sollte sichergestellt werden, dass Datenintermediäre unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse an der Verwertung der verwalteten Daten agieren und dass Interessenkonflikte ausgeschlossen werden. Insbesondere darf die Treuhänderfunktion nicht durch eine Erwerbsabsicht der Datenintermediäre unterminiert werden. Auch müssen finanzielle oder sonstige interessengeleitete Verflechtungen der Datenintermediäre zu anderen privatwirtschaftlichen Akteuren ausgeschlossen sein. Aus Sicht des vzbv wäre die Trägerschaft durch öffentlich-rechtliche Institutionen oder Stiftungen zu bevorzugen, aber auch privatwirtschaftliche Modelle sind denkbar, wenn unter anderem Treuepflichten bestehen, Qualitätsanforderungen festgeschrieben werden und Haftungsfragen geklärt sind.

Diese Treuepflichten der Datenintermediäre gegenüber den Treugebern sollten präzise gefasst werden. Notwendig wären beispielsweise Regelungen zur Zulässigkeit und Grenzen rechtsgeschäftlicher Mandate, insbesondere wenn Datenintermediäre für ihre Nutzer Rechte ausüben, die diesen nach der DSGVO zustehen (zum Beispiel Erteilung von Einwilligungen und ihr Widerruf, Auskunft, Löschung, Datenübertragung, usw.). Darüber hinaus sollten Datenintermediäre besonders hohe Anforderungen an die Transparenz und Angemessenheit von Geschäftsbedingungen erfüllen müssen. Schließlich muss eine potentielle Monopolstellung verhindert sowie Koppelungen unterbunden werden, um auszuschließen, dass etwa ein Anbieter seine Kunden dazu verpflichtet, mit einem bestimmten Treuhänder zusammenzuarbeiten. Wichtig ist weiterhin, Vorkehrungen für den Fall der Insolvenz oder Auflösung zu definieren.

Da die Betroffenen selbst kaum Möglichkeit haben, die Qualität und Zuverlässigkeit von Datenintermediären zu bewerten, sollten gewisse Qualitätsanforderungen gesetzlich festgeschrieben werden. So sollten Vorgaben hinsichtlich der Datensicherheit, insbesondere der Qualität der Verschlüsselung der Daten sowie der Datenübertragungen, aber auch hinsichtlich von Anonymisierungsverfahren entwickelt werden. Notwendig wäre außerdem festzulegen, dass Datenintermediäre zwingend vor Inbetriebnahme die

[16] Vgl. Datenethikkommission der Bundesregierung (2019) (wie Anm. 3), S. 133.

zuständigen Datenschutzaufsichtsbehörden konsultieren und eine Datenschutz-Folgenabschätzung durchführen müssen. Außerdem sollte eine Zertifizierung mit einer entsprechenden Überwachung obligatorisch sein, um zu belegen, dass die Datenintermediäre sowohl organisatorisch als auch technisch in der Lage sind, die Anforderungen zu erfüllen.

Gleichmaßen sollte diskutiert werden, inwieweit Datenintermediäre die Datennehmer überprüfen und deren Zuverlässigkeit gewährleisten müssen. Wichtig ist in diesem Kontext weiterhin, dass Haftungsfragen (abseits der möglichen Verantwortung als datenverarbeitende Stelle) gesetzlich geregelt werden. So muss beispielsweise die Frage geklärt werden, inwieweit auch Datenintermediäre bei einer Datenschutzverletzung durch einen Datennehmer haften sollten. Denkbar wäre beispielsweise auch ein Versicherungszwang zur Absicherung von Ersatzansprüchen der Betroffenen. Auch muss klargestellt werden, inwieweit Datenintermediäre ihre Haftung gegenüber ihren Nutzern vertraglich beschränken können.

Doch auch abseits der Minimierung der Risiken ist ein rechtsicherer Rahmen wichtig, damit Datenintermediäre die erhofften Chancen realisieren können. Beispielsweise muss eine umfassende Kooperation aller Verantwortlichen sichergestellt werden. Da eine solche Zusammenarbeit jedoch nicht immer im Interesse aller Beteiligten ist, wäre eine rechtliche Verpflichtung für Verantwortliche, mit den Datenintermediären zu kooperieren, erwägenswert. Darüber hinaus sollte der Austausch über und die Entwicklung von Interoperabilitäts- und Portabilitätsstandards sowie offenen Schnittstellen gefördert werden.