< Datenmanagement- und **Datentreuhandsysteme** >

Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020

Digital Gipfel 2020

Bundesministerium des Innern, für Bau und Heimat

Schwartmann/Weiß (Hrsg.)

Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020

Version 1.0, 2020

Urheber:
Fokusgruppe Datenschutz
des Digital-Gipfels

Leitung:
Prof. Dr. Rolf Schwartmann
(TH Köln/GDD)
Mitglied der Datenethikkom-
mission der Bundesregierung

Kölner Forschungsstelle
für Medienrecht

Technology
Arts Sciences
TH Köln

Sherpa:
Steffen Weiß
Gesellschaft für Datenschutz
und Datensicherheit e.V.

Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 228 96 96 75 00
info@gdd.de

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Leitung:	Prof. Dr. Rolf Schwartmann	Kölner Forschungsstelle für Medienrecht - TH Köln
Sherpa:	Steffen Weiß, LL.M.	Gesellschaft für Datenschutz und Datensicherheit e.V.
Mitglieder:	Prof. Dr. Christoph Bauer	ePrivacy GmbH
	Patrick von Braunmühl	Bundesdruckerei GmbH
	Susanne Dehmel	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
	Thomas Duhr	Bundesverband Digitale Wirtschaft (BVDW) e.V.
	Philipp Ehmann	eco – Verband der Internet-wirtschaft e.V.
	Dirk Freytag	Bundesverband Digitale Wirtschaft (BVDW) e.V.
	Marina Gehnen	Bundesamt für Sicherheit in der Informationstechnik
	Dr. Stefan Hanloser	ProSiebenSat.1 Media SE
	Maximilian Hermann	Media Broadcast GmbH
	Dr. Robert Hilgers	Bundesdruckerei GmbH
	Dr. Detlef Houdeau	Infineon Technologies AG
	Angelika Hüsch-Schneider	Deutsche Telekom AG
	Frank Ingenrieth, LL.M.	Selbstregulierung Informationswirtschaft e.V.
	Clemens John	United Internet AG
	Dr. Knut Kaulke	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
	Sebastian Kocks, LL.M.	Mediengruppe RTL Deutschland GmbH
	Prof. Dr. Michael Meier	Universität Bonn/Gesellschaft für Informatik e.V.
	Robin L. Mühlenbeck	Kölner Forschungsstelle für Medienrecht - TH Köln
	Dr. Frank Niedermeyer	Bundesamt für Sicherheit in der Informationstechnik
	Frederick Richter, LL.M.	Stiftung Datenschutz
	Katharina Rieke	Bundesverband Digitale Wirtschaft (BVDW) e.V.
	Dr. Sachiko Scheuing	Acxiom Deutschland GmbH
	Achim Schlosser	European netID Foundation
	Sebastian Schulz	HÄRTING Rechtsanwälte
	Dr. Tobias Stadler	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
	Dr. Claus D. Ulmer	Deutsche Telekom AG
	Dr. Martina Vomhof	Gesamtverband der Deutschen Versicherungswirtschaft e.V.
	Rebekka Weiß, LL.M.	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
	Benjamin Walczak	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Geleitwort

Der Digital-Gipfel der Bundesregierung ist eine jährliche Bestandsaufnahme und Standortbestimmung für die Leistungsfähigkeit der Digitalwirtschaft und der Bundesregierung im Bereich der Digitalisierung. Die Fokusgruppe Datenschutz der durch das Bundesministerium des Innern, für Bau und Heimat (BMI) organisierten Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels hat in den Jahren 2017 bis 2019 stufenweise einen Code of Conduct zur Pseudonymisierung personenbezogener Daten entwickelt, der gemeinsam von der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und dem BITKOM als Verhaltensregel gem. Art. 40 DS-GVO eingereicht wird.

Ich persönlich freue mich besonders, dass die Fokusgruppe auch 2020 unter der Herausgeberschaft von Rolf Schwartmann und Steffen Weiß ein Arbeitspapier vorgelegt hat, dass sich mit einem aus Sicht des BMI zentralen Thema für den fairen und datenschutzkonformen Wettbewerb in Deutschland und Europa befasst. Von **Datenmanagement- und Datentreuhandsystemen** zum Zugang zu Netzangeboten versprechen wir uns nicht nur mehr Datenschutz. Es geht auch um die Möglichkeit, deutsche und europäische Standards für faire Single Sign-on-Systeme zu etablieren, die die Nutzerdaten aus den faktisch noch alternativlosen Datentrichtern des Logins der US-Tech-Giganten befreien, um ein gesundes „Daten-Ökosystem“ zu ermöglichen.

Mit dem Arbeitspapier des Jahres 2020 zu „**Datenmanagement- und Datentreuhandsystemen**“ leistet die Fokusgruppe zudem einen wichtigen Beitrag zur Umsetzung der Empfehlungen der Datenethikkommission aus dem Oktober 2019, die sich in ihrer Handlungsempfehlung 21 für den Ausbau praxisgerechter und datenschutzkonformer Datentreuhandsysteme ausgesprochen hat.

Das Papier der Fokusgruppe unter der Schirmherrschaft des BMI liefert damit erneut eine praxistaugliche Orientierungs- und Arbeitshilfe zu einem der zentralen Themen der Digitalisierung. Allen Mitwirkenden der Fokusgruppe aus Wirtschaft, Verwaltung und Wissenschaft gilt im Rahmen des Digitalgipfels unter der Überschrift „Durch Digitalisierung zu mehr Nachhaltigkeit“ mein herzlicher Dank für ihr nachhaltiges Wirken bei der Entwicklung moderner und praxisgerechter Ansätze zur Herstellung fairer Rahmenbedingungen der Digitalisierung.

Berlin, im November 2020

Professor Dr. Günter Krings

Parlamentarischer Staatssekretär im Bundesministerium der Innern,

für Bau und Heimat

Vorwort

„Durch Digitalisierung zu mehr Nachhaltigkeit“ lautet das Motto des Digital-Gipfels 2020. Technische Innovationen zur Unterstützung ökologischer, ökonomischer und sozialer Ziele sind aus Sicht der Bundesregierung wichtige Aspekte eines nachhaltigen Wirkens. Die Digitalisierung bietet auch hier zahlreiche Chancen. Zugleich stellt sich die Frage, wie der Einzelne[1] vor möglichen Fehlentwicklungen wirksam geschützt werden kann. Der Abschlussbericht der von der Bundesregierung im Jahr 2018 eingesetzten Datenethikkommission hält hierfür Antworten bereit und macht Vorschläge, wie der kontrollierte Zugang zu personenbezogenen Daten verbessert werden kann. In diesem Zusammenhang wird insbesondere in **Datenmanagement- und Datentreuhandsystemen** großes Potential gesehen. Grundvoraussetzung hierfür ist, dass solche Systeme praxisgerecht und datenschutzkonform ausgestaltet sind[2]. Sollen die auch von der Datenethikkommission geforderten verstärkten Anstrengungen bei Forschung und Entwicklung solcher Systeme erfolgreich sein, muss in einem ersten Schritt ein gemeinsames Verständnis über Sinn und Zweck solcher Modelle hergestellt werden.

Die Fokusgruppe Datenschutz des Digital-Gipfels möchte hierzu einen Beitrag leisten. In diesem Arbeitspapier für den Digital-Gipfel 2020 werden Modelle von Datenmanagement- und Datentreuhandsystemen dargestellt und erläutert. Um den Praxisbezug zu wahren, werden die Erläuterungen durch bestehende sowie zukünftige Szenarien konkretisiert. Die Fokusgruppe Datenschutz ist davon überzeugt, dass die Fortentwicklung solcher Systeme weiter unterstützt werden muss. Die Wahrung von Transparenz und die angemessene Berücksichtigung der Interessen aller beteiligten Akteure sind dabei von essentieller Bedeutung, sowohl heute, als auch im Rahmen einer künftigen europäischen Regulierung von Datenmanagement- und Datentreuhandsystemen.

Allen Mitwirkenden gebührt herzlicher Dank für die kontinuierliche Arbeit in der Fokusgruppe. Besonders danke ich Herrn Rechtsanwalt Steffen Weiß von der Gesellschaft für Datenschutz und Datensicherheit für die Koordination der Arbeit.

Köln, im November 2020

Professor Dr. Rolf Schwartmann

1 Die in diesem Arbeitspapier gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen.

2 Gutachten der Datenethikkommission, S. 21.

Inhalt

1
Personal Information Management System (PIMS)

1.1 Einleitung 8
1.2 Definitionen von Personal Information Management Systems 9
1.3 Kategorien von Personal Information Management Systems 10
1.4 Effektuierung durch klare Begrifflichkeit 12
1.5 Pseudonymisierung/Anonymisierung 13
1.6 Rolle des Bürgers als „Datengeber“ und Dienste-Nutzer 14
1.7 Praxisbeispiele 15
1.7.1 netID 15
1.7.2 Die elektronische Patientenakte 15
1.7.3 Smart Meter Gateways 16

2
Datentreuhandsysteme

2.1 Einleitung 18
2.2 Definitionen von Datentreuhändern 19
2.3 Anforderungen an Datentreuhänder 21
2.4 Branchenspezifische Anforderungen an Datentreuhänder 22

3
Identitäten – Überprüfung und Verfahren

3.1 Rechtlicher Rahmen im Europäischen Wirtschaftsraum 24
3.2 Modelle von Identitätsmanagementsystemen 26
3.3 Datenschutz bei Identifikationssystemen 27
3.4 Technologien für Identitäten und abgeleitete Identitäten 28
3.5 Umsetzungsmöglichkeiten von Identifikationssystemen 29
3.6 Branchenspezifische Ausgestaltung der Identitätsnachweisqualitäten 30
3.7 Praxisbeispiele 31
3.7.1 Single-Sign-On 31
3.7.2 Advertising Identities 33

Personal Information Management System (PIMS)

1.1

Einleitung

Die Auseinandersetzung mit „Personal Information Management Systems“ oder „Personal Information Management Services“ (abgekürzt jeweils: PIMS), mit Diensten unter Einsatz von „Privacy Enhancing Technology“ (PET) oder mit Einwilligungsmanagement-Systemen (im anglo-amerikanischen Raum teilweise „Privacy Management Tools“ (PMT)) befindet sich in Deutschland noch am Anfang. Auf europäischer Ebene besteht schon länger Aufmerksamkeit. Einer der Ausgangspunkte für eine stärkere Befassung des Datenschutzes mit derartigen Ansätzen ging von der finnischen Initiative MyData seit 2015 aus[3]. Die von der Bundesregierung eingerichtete Stiftung Datenschutz untersuchte im Jahr 2016 verschiedene Ansätze in diesem Bereich[4]. Im September 2016 wurden in einer Stellungnahme des Europäischen Datenschutzbeauftragten die Chancen und Herausforderungen von PIMS bewertet und die Entwicklung solcher innovativen Ansätze gegenüber der EU-Kommission als besonders unterstützenswert hervorgehoben[5]. Neben der Implementierung und Co-Finanzierung durch den öffentlichen Sektor solle auch die Zusammenarbeit mit anderen strategischen Projekten wie der Digital Single Market Strategy und mit Projekten zu Cloud Computing und zum „Internet der Dinge“ intensiviert werden. Der im November 2016 veröffentlichte PIMS-Report der Europäischen Kommission folgte einem bereits 2014 gestarteten Konsultationsprozess und setzte sich eingehend mit den besonderen Herausforderungen bei der Implementierung von PIMS-Plattformen auseinander[6]. Auf nationaler Ebene haben die Regierungsparteien im Koalitionsvertrag 2018 eines der Anwendungsziele des PIMS-Ansatzes adressiert und vereinbart, dass man die Entwicklung von innovativem Einwilligungsmanagement fördern und unterstützen wolle[7]. In Umsetzung dessen finanzierte das BMJV von Sommer 2019 bis Frühjahr 2020 ein entsprechendes Projekt[8]. Die Datenethikkommission der Bundesregierung brachte der Thematik mit der ausführlichen Erwähnung in ihrem Gutachten 2019 mehr Sichtbarkeit[9].

PIMS-bezogene Angebote werden als aufstrebender Markt betrachtet. Für einige Beobachter haben PIMS das Potential, herkömmliche Praktiken der Sammlung und Nutzung personenbezogener Daten zu revolutionieren. Im Zentrum steht dabei, wie durch die Nutzung von PIMS die Kontrolle und Verwaltung von Identitäten, Einwilligung und Präferenzen der Datennutzung verändert und weiterentwickelt werden kann. Der Rahmen für diese Entwicklung wird durch die EU-Datenschutzgrundverordnung (DS-GVO) vorgegeben. PIMS müssen die darin festgelegten Grundprinzipien, aber auch konkrete Vorgaben wie die Wirksamkeitsvoraussetzungen einer Einwilligung oder die Einführung des „Privacy by Design and by Default“ hinreichend berücksichtigen.

---

[3] “MyData – A Nordic Model for human-centered personal data management and processing” (Whitepaper, 2015), http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=y

[4] “Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen”, Studie 2016/2017, https://stiftungdatenschutz.org/themen/pims-studie

[5] EDPS Opinion on Personal Information Management Systems: “Towards more user empowerment in manag-ing and processing personal data”, https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en

[6] “An emerging offer of “personal information management services” - Current state of service offers and chal-lenges”, https://ec.europa.eu/digital-single-market/en/news/emerging-offer-personal-information-management-services-current-state-service-offers-and

[7] Koalitionsvertrag zwischen CDU, CSU und SPD, April 2018, S. 47, www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906

[8] PM zum Abschlussbericht der Studie „Innovatives Datenschutz-Einwilligungsmanagement“, September 2020, https://bmjv.de/SharedDocs/Downloads/DE/News/PM/090720_Datenschutz.html

[9] Gutachten der Datenethikkommission, S. 133, www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenethikkommission/arbeitsergebnisse-der-dek/arbeitsergebnisse-der-dek-node.html

1.2

Definitionen von Personal Information Management Systems

Eine allgemeine Definition von Personal Information Management Systems existiert nicht; die Begrifflichkeit ist rechtlich nicht geschützt und wird für unterschiedliche daten- und datenschutzbezogene Dienstleistungen genutzt. Die verschiedenen Dienste und Systeme lassen sich übergreifend beschreiben als eine technologiegestützte Anwendung zum Aufbau von Ökosystemen, mit deren Hilfe Personen in die Lage versetzt werden, die Sammlung und Verarbeitung, die Verbreitung sowie den Austausch ihrer persönlichen Daten besser zu überblicken und zu steuern. Die Datensouveränität als Zielstellung des PIMS-Ansatzes wird auch in Erwägungsgrund 7 Satz 2 DS-GVO als tragendes Motiv benannt: „Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen."

Die meisten PIMS-Ansätze sind Instrumente des Selbstdatenschutzes. Sie zielen darauf ab, die Datensouveränität des Einzelnen zu stärken und die Ausübung von Datenschutzrechten zu erleichtern. Betroffene werden ertüchtigt, die Verbreitung und Nutzung ihrer personenbezogenen Daten besser zu kontrollieren und (alternativ oder kumulativ) ihre Online-Identität zu verwalten. Ein solches nutzerorientiertes Einwilligungsmanagement ist für alle beteiligten Akteure vorteilhaft. Betroffenen wird die Entscheidung, welche Daten zu welchen Zwecken preisgegeben werden sollen, deutlich erleichtert. PIMS haben insoweit auch das Potential, ungleiche Machtverhältnisse wieder einander anzugleichen. Datenverarbeiter hingegen haben bei Einsatz von PIMS einen standardisierten Zugang zu den betroffenen Personen und damit eine einfachere Möglichkeit, Betroffene zu der Abgabe einer Einwilligung zu bewegen. Hierdurch verringert sich für Datenverarbeiter nicht nur der Verwaltungsaufwand. Die datenschutzkonforme Ausgestaltung des Prozesses ermöglicht vielmehr die bestmögliche Erfüllung der durch die DS-GVO geforderten Nachweispflicht und steigert so die Rechtssicherheit insgesamt.

1.3

Kategorien von Personal Information Management Systems

Da sich PIMS-Angebote noch immer in einem frühen Entwicklungsstadium befinden, weichen die in den jeweiligen Modellen verfolgten Konzepte und Geschäftsmodelle stark voneinander ab. Hintergrund ist, dass Größe und Beschaffenheit des zu erschließenden Marktes noch auszuloten sind. Nur vereinzelt existieren bereits Erfahrungen zur praktischen Anwendung und zu (positiven) Auswirkungen auf die Verarbeitung personenbezogener Daten.

Ungeachtet des von allen Ansätzen verfolgten Ziels einer Steigerung der Nutzerkontrolle bestehen in der Architektur der Dienste die folgenden grundsätzlichen Unterschiede:

Datenspeicherung:

- Werden überhaupt Daten erhoben/aggregiert und im PIMS gespeichert oder beschränkt sich der Dienst auf Verlinkung/Aufbau eines Zugriffs- bzw. Übermittlungsmanagements ohne eigene Datenhaltung unter Belassung der Datenbestände am jeweiligen Speicherort (z.B. auf dem Nutzer-Endgerät)?

- Haben datennutzende Akteure aus dem privaten oder öffentlichen Sektor direkten Zugriff auf die Daten (passiver Intermediär) oder erfolgt eine Freigabe nach inhaltlicher Zugriffskontrolle durch das PIMS (aktiver Intermediär)?

- Werden unter der Zugriffskontrolle des PIMS Klardaten an datennutzende Akteure übermittelt oder werden lediglich Substrate/Score-Werte/Analyseergebnisse übermittelt?

- Werden im Falle einer tatsächlichen Datenhaltung durch das PIMS die Daten zentral beim Dienstanbieter auf dessen Server/in dessen Cloud gespeichert oder werden Daten dezentral auf dem Nutzer-Endgerät oder als Mischvariante in zentral vorgehaltenem aber separiertem/nutzerspezifischem Speicherort („personal cloud“)?

Hinsichtlich der Funktionalität lassen sich PIMS-Angebote grob wie folgt unterteilen:

Datenspeicher: Nutzerzentrierte Cloud-Angebote hauptsächlich zur **Speicherung persönlicher Daten** (“personal data space”/“personal data safe“/” data vault“/„data locker“), u.U. ergänzt durch Analysefunktionen oder die Möglichkeit, personenbezogene Daten über die eigene Person zu vermarkten.

- **Praxisbeispiel:** *Cozy Cloud*[10]
- **Praxisbeispiel:** *ownCloud*[11]/*Nextcloud*[12]
- **Praxisbeispiel:** *Weople*[13]
- **Praxisbeispiel:** *DataVaults*[14]

Daten-Cockpits: Auf **Überblick, Transparenz und Kontrolle abzielende Angebote** („privacy dashboard", „Daten-Cockpit"), die über eine Webseite oder installierte Applikation eine Datenzugriffs- und Datennutzungskontrolle der einzelnen Person ermöglichen; teils auf hochgranularer Ebene in Bezug darauf, auf welche Daten (oder Teilmengen von Daten) von wem wann wie oft und zu welchem Zweck zugegriffen werden kann.

Einwilligungsmanagement-Dienste: Erleichterung der jederzeitigen Erteilung oder des Widerrufs von Einwilligungserklärungen zur Datenverarbeitung („dynamic consent"), so u.a. hinsichtlich der Zwecke, und der Empfänger von personenbezogenen Daten.

- **Praxisbeispiel:** *Transparency & Consent Framework des IAB Europe*[15]
- **Praxisbeispiel:** *netID (so auch im Bereich der PIMS und des Identitätsmanagements, vgl. Ziff. 1.6.1)*
- *Usercentrics*[16]

Datenschutz-Assistenten („privacy agent"): Zur treuhänderischen Umsetzung und Durchsetzung individueller Nutzerpräferenzen, speziell zur Erteilung und Widerruf von Einwilligungen und Ausübung der Betroffenenrechte (Auskunft, Löschung, Berichtigung, Portierung) im Auftrag des Datensubjekts; ein Unterfall können PIMS-Angebote zur **Unterstützung einzelner Betroffenenrechte sein**, z.B. Auskunftsmanagement, Portabilitätsmanagement.

Identitätsmanagement: **Dienste zur Verwaltung digitaler Identitäten, ggf. als sog.** „Single-Sign-On-Lösung" (vgl. Ziff. 3.7.1).

- **Praxisbeispiel:** *Jolocom*[17]

Die oben genannten typischen **PIMS**-Funktionalitäten können auch kombiniert angeboten werden:

- **Praxisbeispiel:** *digi.me*[18]
- **Praxisbeispiel:** *Meeco*[19]

[10] https://cozy.io
[11] https://owncloud.com/de/
[12] https://nextcloud.com/
[13] https://weople.space/en/#functions
[14] FraunhoferFOKUS-H2020-Projekt DataVaults, www.datavaults.eu
[15] https://iabeurope.eu/transparency-consent-framework/
[16] https://usercentrics.com/de/website-consent-management
[17] https://jolocom.io/solution
[18] https://digi.me
[19] www.meeco.me

1.4

Effektuierung durch klare Begrifflichkeit

Die noch nicht standardisierte Verwendung des Begriffes PIMS und die Vielzahl der Einsatzszenarien birgt derzeit die Gefahr nicht kongruenter Erwartungen sowohl auf Datengeber- als auch Datennehmerseite. Hieraus resultierende Enttäuschungen sollten vermieden werden. Effektiver Datenschutz wird bereits teils als unnötige Bürokratie ohne Mehrwerte für Betroffene betrachtet. Dieser Eindruck entsteht und verstetigt sich umso leichter, je häufiger Fehlerwartungen gesetzt und sodann enttäuscht werden.

Ausschließlich am Begriff „Personal Information Management" angelehnt, erscheint ein breites Verständnis auch im Sinne der Souveränität der Betroffenen zielführend. Allerdings sollte der für Nutzer breite und mehrwertige Anwendungsbereich des Managements von auf anderen Rechtsgrundlagen als der Einwilligung gestützter Datenverarbeitungen weiter gestärkt werden. Zugleich birgt eine Konfusion derartiger Management-Systeme mit der Begrifflichkeit der Einwilligung die Gefahr, dass sich der Irrglaube, Datenverarbeitungen bedürften stets einer Einwilligung, weiter verstetigt. Hierbei bieten PIMS auch und gerade im Kontext der Betroffenenrechte nach Art. 12 ff. DS-GVO und insbesondere im Kontext des Widerspruchsrechts nach Art. 21 DS-GVO[20] gegen gewisse Verarbeitungen auf der Grundlage eines berechtigten Interesses große Potentiale.

Hieraus ergeben sich nachstehende Korrelationen zwischen Rechtsvorgaben und Anwendungsszenarien:

- **Artikel 7 i.Vm. Artikel 5 DS-GVO:** Einwilligungsmanagement
- **Artikel 21 DS-GVO:** Widerspruchs-Managements und ggf. eines Opt-In Managements, hier verstanden als Widerrufs eines zunächst erteilten Widerspruchs[21]
- **Artikel 15, Artikel 16, Artikel 17 DS-GVO, eIDAS Verordnung:** Personal Identity Management
- **Artikel 15, Artikel 16, Artikel 17, Artikel 20 DS-GVO:** Personal Data Management

Funktionalitäten und rechtliche Kontexte können sich selbstverständlich gegenseitig ergänzen und überschneiden.

Eine Systematisierung der Dienste ermöglicht sodann auch die Entwicklung branchenspezifischer Umsetzungen, die weitere Mehrwerte für Betroffene bilden können. Dieses Dokument geht im Weiteren auf mehrere Themen ein, etwa Datentreuhänder, SSO-Dienste, Advertising Identities. Branchenspezifische, weitere Ausgestaltungsmöglichkeiten des Verständnisses und der Anforderungen, auch unter Berücksichtigung der Integration von PIMS, liegen auf der Hand. In den jeweiligen Kapiteln wird ein kurzer Ausblick auf diese Möglichkeiten gegeben.

[20] Beachte insb. Art. 21 Abs. 5 DS-GVO.

[21] Ein Opt-In ist hier verstanden als die Umkehr eines (vorher ausgeübten) Widerspruchs (Opt-Outs).

1.5

Pseudonymisierung/ Anonymisierung

Abhängig von der jeweiligen Funktionalität eines PIMS (siehe 1.3) kann dieses auch dazu dienen, dass Betroffene im Falle einer Verarbeitung pseudonymisierter bzw. anonymisierter Daten ein gewisses Maß an Kontrolle erhalten.

Gerade als branchenspezifische Lösung können PIMS für die Betroffenen eine Möglichkeit bieten, den vielfältigen Einsatz von pseudonymisierten Daten im Blick zu behalten. Zum Beispiel im Bereich der medizinischen Forschung kann dies relevant sein, damit die Betroffenen auch zu einem späteren Zeitpunkt ihre Auskunftsrechte und Rechte auf Korrektur oder Löschen gegenüber allen durchsetzen können, die mit den Daten gearbeitet haben.

Die PIMS können als Treuhänder agieren und den Betroffenen einen Überblick darüber verschaffen, welche Daten bereits pseudonymisiert bzw. anonymisiert verwendet werden. Nur mit diesem Überblick kann die Gefahr einer Re-Identifizierung abgeschätzt werden bzw. mithilfe des PIMS könnten Mechanismen zum Einsatz kommen (statistisches Rauschen, Dummy-Einträge, synthetische Daten), mit denen eine Re-Identifizierung erschwert oder verhindert werden kann.

Diese Mechanismen im Sinne von Differential Privacy können dann einen wirksamen Schutz bieten, wenn sie sowohl bei der Generierung eines Datensatzes für eine Nutzung zum Einsatz kommen als auch für die einzelnen Betroffenen alle Nutzungen über einen längeren Zeitraum verwalten. Re-Identifizierungen durch Schlussfolgern oder Verknüpfen mit mehreren Datensätzen können auf diese Weise verhindert werden.

1.6

Rolle des Bürgers als „Datengeber“ und Dienste-Nutzer

Der Ansatz und dogmatische Ausgangspunkt des Konzepts der Personal Information Management Systems/Services entspricht der deutschen Rechtsfigur der informationellen Selbstbestimmung. Das europäische verankerte Recht auf Datenschutz soll durch PIMS ergänzt werden um ein Instrument der Datenkontrolle. Über die gesetzlich garantierten Betroffenenrechte hinaus will der PIMS-Ansatz die Nutzerinnen und Nutzer vom Datenobjekt („Betroffener“) zum Datensubjekt entwickeln und auf diese Weise digitale Souveränität fördern. Der von der finnischen Initiative MyData entwickelte Leitgedanke (“*empowering individuals and create a human centric data economy*”) soll ein Verständnis stärken, nach welchem die Verbraucherinnen und Verbraucher als respektierte Datengeber auftreten. Gegenüber Wirtschaftsakteuren und Behörden als Datennutzern sollen Betroffene an Verhandlungsmacht und Durchsetzungsvermögen gewinnen. Dies soll sowohl den Datenschutz im engeren Sinne befördern (DS-GVO-Vorgaben, speziell hinsichtlich informierter Einwilligung) als auch wirtschaftliche Machtungleichgewichte und Informationsasymmetrien mindern. Datenschutzrechte sollen von einer teils schwer verständlichen Rechtsmaterie mit bürokratischen Mechanismen im Idealfall zu “Ein-Klick-Rechten” werden. Die hierfür notwendige Plattform und das technische Umfeld sollen zukünftig PIMS-Angebote bereitstellen.

1.7

Praxisbeispiele

1.7.1 netID

Im Kontext der PIMS nimmt die netID mehrere der beschriebenen Rollen/Funktionen ein. Es bietet für Nutzer sowohl eine Single-Sign-On Funktionalität an (vgl. Ziff. 3.7.1), als auch die Möglichkeit zur Verwaltung von Einwilligungserklärungen, die Nutzer gegenüber einem digitalen Dienst erteilt haben. Beispielsweise kann ein Nutzer seine Einwilligung erteilen, auf Basis einer abgeleiteten pseudonymisierten ID personalisiert angesprochen zu werden.

Beide Funktionen (SSO, Einwilligungsmanagement) können seitens eines Dienstes parallel aber auch getrennt zur Verwendung angeboten werden. Die Entscheidung obliegt dabei stets dem Nutzer. Die netID agiert im Verhältnis zum Betroffenen passiv bzw. neutral. Das bedeutet, dass sie immer das Verhältnis zwischen dem Nutzer und einem anderen digitalen Dienst (netID Partner) regelt, so bspw. die Erlaubnis zur dortigen Einblendung personalisierter Anzeigen. Nutzer verwenden ihren netID-Account zum einen, um im Rahmen eines Single-Sign-On geräteunabhängig die Autorisierung von Datenübertragungen an Dienste zu verwalten und um Änderungen an ihren Privatsphäre-Einstellungen vorzunehmen, hier insbesondere die Verwaltung von Einwilligungserklärungen bzgl. der Datenverarbeitungen durch einen anderen Dienst.

Wesentliche Vorteile ergeben sich hierbei für Nutzer, da diese ihre Privatsphäre-Einstellungen an zentraler Stelle dauerhaft und unabhängig vom Endgerät vornehmen können. Wiederholte Ansprachen zwecks des Einholens von Einwilligungen und eine daraus resultierende „Consent-Fatigue“ werden ebenfalls vermieden.

1.7.2 Die elektronische Patientenakte

In der deutschen Gesundheitsversorgung entstehen täglich tausende Vorsorge-, Diagnose und Therapie-Daten von Patienten, erzeugt von Ärzten und Arzthelfern, in Krankenhäusern oder Kliniken. Ein Kernstück der Digitalisierung soll die Erzeugung der elektronischen Patientenakte (ePA) sein. Ab dem Jahr 2021 sollen personenbezogene Daten von über 73 Millionen gesetzlich Versicherten auf Basis deren Einwilligung in einer ePA zentral gespeichert werden. Nach dem Terminservice- und Versorgungsgesetz (TSVG) und insbesondere nach dem Patientendatenschutz-Gesetz (PDSG) kann die ePA Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte, Impfungen, elektronische Medikationspläne, elektronische Arztbriefe und Notfalldatensätze enthalten. Dadurch sollen u.a. wichtige Daten schneller verfügbar, Mehrfachuntersuchungen und Medikationen mit gegengesetzten Wirkungen vermeidbar, sowie der Patientenzugang auch mobil erfolgen können.

Mit Blick auf die unterschiedlichen Funktionalitäten der PIMS steht den Betroffenen bei der ePA ein persönlicher Datenspeicher, ein Daten-Cockpit sowie ein Dienst zum Einwilligungsmanagement zu Verfügung. Eine granulare Steuerungsmöglichkeit der Betroffenen, welcher Empfänger auf konkret

welches Datum (z.B. Arztbriefe) zugreifen darf, ist allerdings erst in einer erweiterten Entwicklungsstufe der ePA möglich, was die Datenschutzkonferenz bereits zu Kritik am Gesetzesentwurf veranlasst hat[22]. Insofern wird es für PIMS insbesondere im Gesundheitsbereich wichtig sein, den Betroffenen möglichst detailliert die Verwaltung von einzelnen Datensätzen oder Einwilligungserklärungen zu ermöglichen, um einen Beitrag zu mehr Nutzerkontrolle leisten zu können.

Um die Qualität der ärztlichen Vorsorge, Diagnose und Therapie künftig zu erhöhen und um gleichzeitig die Vielzahl an wissenschaftlichen Forschungsergebnissen (ca. 6000 Publikationen weltweit pro Tag) automatisiert auszuwerten, werden künftig KI-Assistenz-Systeme für unterschiedliche Anwendungen entstehen und Ärzten in Deutschland zur Verfügung gestellt. Diese KI-Assistenzsysteme werden immer genauer und damit wertvoller, je mehr Trainingsdaten einfließen. Der Gesetzgeber sieht dazu freiwillige „Datenspenden" von Patienten vor, die zunächst anonymisiert und dann zum KI-System für die „Weiterentwicklung" transferiert werden sollen. Auch hier können PIMS ihren Beitrag leisten, indem den Betroffenen transparente und nachvollziehbare Steuerungsmöglichkeiten über ihre Daten zur Verfügung gestellt werden.

1.7.3 Smart Meter Gateways

In intelligenten digitalen Messsystemen bilden sog. „Smart Meter Gateways" die zentrale Komponente, die Messdaten von Zählern von Verbrauchern empfängt, speichert und für beteiligte Marktakteure aufbereitet. Damit einhergehend ist ein erhöhter Datenverkehr, der Aufschluss über das Verbrauchsverhalten geben kann. Als Schnittstelle zwischen dem Verbraucher und den Marktakteuren verfügen Smart Meter Gateways über eine PIMS-Funktionalität, um den Nutzern, Datenflüsse zu generierten Zählwerten aus der häuslichen Verbrauchsmessung (Energie, Wärme, Wasser) transparent darzustellen. Mittels Datenzugriffsprofilen wird ferner aufgezeigt, welche Stelle wann welche Daten für gesetzlich gebotene Fälle erhält[23].

[22] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), Entschließung vom 01.09.2020

[23] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1 - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Ziff. 4.2.2.1.1.

Datentreuhandsysteme

2.1

Einleitung

Die Corona-Krise hat vor Augen geführt, welche herausragende Bedeutung aktuelle und qualitativ hochwertige Daten für Gesellschaft und Wirtschaft haben können. Auf politischer Ebene wird über die sowohl von der Bundesregierung als auch von der EU erarbeiteten Datenstrategien daran gearbeitet, Daten besser nutzbar zu machen und im Rahmen der Vorgaben der DS-GVO den Zugang und die Verteilung von Daten zu verbessern.

Im Zuge der Diskussionen rund um die neue Datenpolitik geraten auch die sogenannten Datentreuhänder immer stärker in den Fokus. Mit ihnen werden Potenziale für verbessertes Datenteilen, mehr Nutzersouveränität und niedrigschwelligen Datenzugang verbunden. Wie Datentreuhandsysteme funktionieren können, welche Kategorien unterschieden werden sollten und welche datenschutzrechtlichen Fragestellungen[24] auftreten können, soll in den folgenden Abschnitten dargestellt werden. Dies soll vor allem zur stärkeren Strukturierung des Diskurses beitragen, die zur Klärung der offenen (Rechts-)Fragen unerlässlich ist.

[24] Bei der Betrachtung von Datenzugangsrechten und der Verteilung von Daten spielt nicht nur das Datenschutzrecht eine entscheidende Rolle. Daneben sind z.B. Investitionsschutz, Geschäftsgeheimnisschutz, Wettbewerbsrecht, Urheberrecht zu beachten. Hierzu ausführlich: https://www.bitkom.org/Bitkom/Publikationen/Rechtsfragen-der-digitalisierten-Wirtschaft-Rechte-an-Daten.

2.2

Definitionen von Datentreuhändern

Eine feststehende Definition von Datentreuhändern hat sich noch nicht etabliert. Diskutiert wird bislang eher der Einsatz bzw. die Zielstellung solcher Systeme. In einem Themenpapier zu Datentreuhändermodellen[25] werden richtigerweise verschiedenste Zielstellungen kategorisiert, die mit Datentreuhändern verwirklicht werden sollten. Sie lassen sich in vier Bereichen zusammenfassen:

- Stärkung und Förderung der Nutzersouveränität im Datenökosystem (z.B. PIMS)
- Förderung des Datenaustauschs und der Zugänglichmachung von Daten hoher Qualität (z.B. Datenplattformen)
- Unparteiliche und transparente Datenverwaltung (z.B. Intermediäre)
- Verbesserung der Wettbewerbsbedingungen und zugleich Stärkung europäischer Plattformen

Um eine Klärung und Konkretisierung der Datentreuhänder weiter anzustoßen, bietet sich eine Befassung mit ihren Rollen und Funktionen an. Datentreuhänder stehen als Intermediär in einer Datenvermittlerrolle zwischen den Nutzergruppen: Datengeber und weitere Dritte (z.B. Datennutzer). Die Rolle und Aufgabe der Treuhänder umfasst in einer solchen Konstellation beispielsweise die sichere „Verwahrung", also Speicherung der Daten zum Zwecke der späteren, vereinbarungsgemäßen Weitergabe. Dies könnte beispielsweise in einer Datenplattform zur Nutzbarmachung von Patientendaten erfolgen[26]. Der Patient würde in einer solchen Fallgestaltung ausgewählte Daten bereitstellen, die z.B. in einer Studie anfallen und die Nutzung für Dritte nach vorbestimmten Kriterien oder für bestimmte Empfänger (z.B. Forschungseinrichtungen) freigeben[27]. Über Maßnahmen wie Pseudonymisierung und Schlüsselverwaltung seitens der Treuhänder könnte in einem solchen Modell der Zugang und die Nutzung von Patientendaten verbessert werden, ohne dass die Identität des Patienten dem Datennutzer offengelegt werden muss. Die Identifizierung und damit die Zuordnung der Daten zu einer bestimmten Person wäre nur dem Treuhänder möglich. Ihm kommt dadurch eine besondere Vertrauensstellung zu.

Eine weitere Aufgabe des Treuhänders kann beispielsweise darin bestehen, die übermittelten Daten auf Integrität zu prüfen und die jederzeitige Identifizierbarkeit des Datengebers sicherzustellen. Dies dient beispielsweise auch der Durch- und Umsetzung von Betroffenenrechten sowie dem Einwilligungsmanagement. Daneben sind weitere Leistungen wie Datenaufbereitung denkbar.

Einsatzfelder der Datentreuhänder werden auch beim Zugang zu Leistungen der öffentlichen Hand, im Kontext des Identitäts- oder Einwilligungsmanagements über eine neutrale Stelle und

[25] Von April 2020, erarbeitet von: Aline Blankertz, Stiftung Neue Verantwortung, Berlin; Patrick von Braun-mühl, Bundesdruckerei, Berlin; Pencho Kuzev, Konrad-Adenauer-Stiftung, Berlin; Frederick Richter, Stif-tung Datenschutz, Leipzig; Heiko Richter, Max-Planck-Institut für Innovation und Wettbewerb, München; Martin Schallbruch, Digital Society Institute, ESMT Berlin, im Folgenden kurz: „Themenpapier Datentreu-handmodelle" genannt.

[26] Nicht alle diskutierten Fallkonstellationen umfassen die Speicherung der Daten beim Treuhänder selbst. Er kann sich dafür einerseits Dritter bedienen oder auch in einer Art und Weise fungieren, dass er lediglich die Datenteilungsbereitschaft der Nutzer verwaltet und ggf. die nutzenden Parteien miteinander vernetzt, die Datenfreigabe selbst also zu gegebener Zeit vom Nutzer selbst erfolgt.

[27] In dieser Fallkonstellation wird häufig auch das Konstrukt der sogenannten Datenspende benannt, auf das hier aber nicht näher eingegangen werden soll.

für die Datenverteilung zwischen Wirtschaftsakteuren gesehen. Dabei kann regelmäßig zwischen B2C-Treuhändern und B2B-Treuhändern unterschieden werden. Während bei einem B2C-Treuhänder Daten von Verbrauchern durch den Treuhänder gespeichert oder vermittelt werden, bieten B2B-Treuhänder ihre Leistungen gegenüber Wirtschaftsakteuren oder anderen Verantwortlichen an.

Auch der Treuhandbegriff selbst bedarf der Konkretisierung, da die verschiedenen Fallkonstellationen von einem Dienstleistungsansatz (Datenmanagement), der vor allem gegenüber dem Datengeber verpflichtet ist, bis hin zu einem „echten" Intermediär reichen, der gegenüber allen angeschlossenen Parteien Verantwortung übernimmt[28]. Gerade beim Dienstleistungsansatz zeigt sich, dass eine klare Trennung zwischen den PIMS und den Treuhändern nicht immer möglich ist. Insofern können Mischformen bestehen, bei denen ein PIMS auf Basis eines Datentreuhandmodells angeboten wird. Der Begriff der Datentreuhand ist im Übrigen datenschutzrechtlich autonom zu bestimmen. Treuhandmodelle außerhalb des Datenschutzrechts, etwa die fiduziarischen Pflichten des Treuhänders gegenüber dem Treugeber im Zivilrecht, sind instruktiv aber datenschutzrechtlich nicht bindend.

Für den Erfolg und die Erreichung der beschriebenen Ziele mit Datenmanagement- und Datentreuhandmodellen ist es notwendig, ihre Aufgaben jedoch weiter zu konkretisieren und vor allem auch gemeinsam mit der Wirtschaft Praxisbeispiele zu etablieren. Hierbei sind auch vorhandene Marktlösungen, die den Verbraucher in der Rechte- und Zugriffszuweisung sowie dem Handling seiner Daten unterstützen, zu beachten und ggf. auf diesen aufzusetzen. Ferner sollte geklärt werden, in welchen Sektoren sich Treuhandmodelle anbieten, ob die entsprechende Plattform staatlich oder privatwirtschaftlich betrieben werden soll und ob das Treuhandmodell selbst die Daten verwalten oder eher Zugriffe auf weitere Datenbanken ermöglichen soll.

[28] So beispielsweise im Rahmen der Pseudonymisierung personenbezogener Daten, vgl. Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, S. 40.

2.3

Anforderungen an Datentreuhänder

Im Rahmen der „sicheren" Speicherung und Schlüsselverwaltung, beispielsweise von pseudonymisierten Daten, muss der Treuhänder stets auch die Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 24 DS-GVO gewährleisten. Da die konkreten Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken gewählt werden müssen, ist es unerlässlich, dass der Treuhänder die Daten entweder entsprechend kategorisiert oder Sicherheitsmaßnahmen umsetzt, die allen Datengruppen gerecht werden.

Im Verhältnis zwischen Intermediär (Datentreuhänder) und den nutzenden Parteien muss der Treuhänder vor allem Transparenz herstellen über seine Rolle, den Funktionen seiner Leistungen und den konkreten Aufgabenzuweisungen. Es sind dabei unterschiedliche Konstellationen wie Auftragsverarbeitungen (Art. 28 DS-GVO), getrennte oder auch gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) grundsätzlich denkbar. Bei der Abgrenzung dieser unterschiedlichen Konstrukte wird es im Einzelfall zu untersuchen sein, inwieweit der Treuhänder nach eigenem Ermessen über Zwecke und Mittel der Verarbeitung bestimmt.

Mit Blick auf die Schlüsselrolle der Datentreuhänder im Rahmen der Zugänglichmachung von personenbezogenen Daten bedarf es der Ausarbeitung besonderer Anforderungen an ihre Zuverlässigkeit. Hierzu sollten gemeinsam mit der Wirtschaft Verfahren zur Zertifizierung von Treuhändern entwickelt werden, um die Stellung als Vertrauensanker zu stärken und Rechtssicherheit für alle Teilnehmer am Treuhandsystem zu schaffen. Darüber hinaus sollte untersucht werden, ob es weitere Rahmenbedingungen bzw. eine Regulierung für die Zulassung von Datentreuhändern in bestimmten Bereichen geben muss, um die Marktentwicklung zu fördern. Entsprechende Regelungen könnten insbesondere Mindestanforderungen, Kontrollmechanismen und Vorgaben zur Intermediärsstellung umfassen[29]. Sollte ein Datentreuhänder beispielsweise im Bereich der PIMS eingesetzt werden, sind Interessenskonflikte des Treuhänders auszuschließen.

[29] Vgl. auch Themenpapier Datentreuhandmodelle, dort insbesondere auch „Neutralitätsgebot".

2.4

Branchenspezifische Anforderungen an Datentreuhänder

Branchenspezifische Anforderungen sind in mehreren Dimensionen möglich. Einerseits anhand der eigentlichen Funktion eines Datentreuhänders. Je mehr ein Datentreuhänder die Rolle eines neutralen Vermittlers einnimmt, umso größer werden die Erwartungen der Betroffenen und entsprechend sollten auch die Anforderungen steigen.

Andererseits kann, orientiert an den konkreten Einsatzszenarien, eine weitere Ausgestaltung zielführend sein. Einerseits auf technischer Ebene, um etwa hochspezialisierte Anforderungen eines Subsektors auf technischer Protokollebene zu adressieren. Oder aber auch auf technisch-organisatorischer Ebene, um etwa unterschiedliche Vertrauensgrade je treuhänderisch verwalteter Daten zu adressieren. So erwarten Betroffene zu Recht im Kontext der Verwaltung sensibler medizinischer Informationen oder sonstiger mit erhöhten Risiken einhergehenden Informationen, wie etwa Bank- und Kreditkartendaten, eine besondere Eignung des Datentreuhänders.

Identitäten – Überprüfung und Verfahren

3.1

Rechtlicher Rahmen im Europäischen Wirtschaftsraum

In der „analogen Welt“ gibt es in den EU Mitgliedsstaaten keine einheitlichen gesetzlichen Regelungen zu Identitätsdokumenten. Es gibt Staaten, die z.T. seit mehr als 60 Jahren keine Ausweispflicht besitzen, wie Großbritannien, Frankreich und Schweden. Es gibt Staaten, in denen eine Ausweispflicht ab dem 16. Lebensjahr besteht, wie in Deutschland, allerdings reicht ein Reisepass oder Personalausweis. Es gibt Staaten mit verpflichtender Identitätskarte, wie Italien und Spanien und es gibt mit Estland einen Staat, der bereits im Jahr 2006 eine verpflichtende elektronische Identitätskarte mit elektronischer Signaturfunktion eingeführt hat[30] .

In der „digitalen Welt“ existiert der Begriff des elektronischen Identitätsnachweises, siehe z.B. § 18 Personalausweisgesetz (PAusG) in Deutschland. Um in allen EU-Mitgliedsstaaten die elektronischen Identitäten und die damit verbundenen Vertrauensdienste gegenseitig anzuerkennen, wurde die Verordnung (VO) 910/2014 am 23.07.2014 „eIDAS-Verordnung“) beschlossen. Auch auf nationaler Ebene setzen gesetzliche Initiativen auf ein interoperables Nutzermanagement, so beispielsweise das Onlinezugangsgesetz (OZG).

Die Regulierung einer „europäischen Identität“ ist damit nicht erforderlich. Die EU-Kommission hat es sich dennoch zum Ziel gesetzt, eine solche Identität vorzuschlagen[31].

In Artikel 9 der eIDAS-Verordnung ist beschrieben, wie ein nationales Identifizierungssystem bei der EU-Kommission notifiziert werden kann, um so von allen anderen Mitgliedsländern anerkannt zu werden. Bis August 2020 haben 15 EU-Mitgliedstaaten mindestens eine Notifizierung erlangt. Die Liste wird von der EU-Kommission veröffentlicht, regelmäßig aktualisiert und enthält eine Angabe zum erzielten Sicherheitsniveau (level of assurance)[32]. Die Anwendungsbereiche reichen vom öffentlichen Sektor (e-Government) über den halböffentlichen Sektor (z.B. ÖPNV), bis zum privaten Sektor (e-Business).

Beispiel für eine eIDAS-Anwendung im G2B-Bereich: *Ein Straßenausbau wird im Land A öffentlich ausgeschrieben. Ein Bauunternehmer aus Land B gibt mit seinem elektronischen Ausweis im Land A ein verbindliches Angebot im Online-Verfahren ab.*

[30] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[31] https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_20_1655

[32] Detlef Houdeau, Tina Hühnlein, Klaus-Dieter Wolfenstetter, Digitale Identität als Fundament der vertrauenswürdigen Transformation, Zeitschrift DuD, Heft 1, 2019

Beispiel für eine eIDAS-Anwendung im G2C-Bereich: *Ein Student im Land C bucht im Land D ein Gastsemester im Online-Verfahren[33]. Sowohl der Identitäts- als auch der Studien- bzw. Qualifikationsnachweis erfolgen dabei elektronisch.*

Die Festlegung unterschiedlicher Sicherheitsniveaus für Identifizierungssysteme in der eIDAS-Verordnung (vgl. Art. 8) und der technologieneutrale Bewertungsrahmen für die Vertrauenswürdigkeit eines Identitätsmittels verdeutlichen, dass die Anforderungen an das Identitätsmittel regelmäßig von ihrem Einsatzzweck abhängig sind. Gleichzeitig wird mit der eIDAS-Verordnung und mit dem OZG ein Interoperabilitätsrahmen geschaffen, bei dem die Einführung einer übergreifenden Identität nicht notwendig ist.

[33] https://www.erasmuswithoutpaper.eu/

3.2

Modelle von Identitäts-managementsystemen

Bisher gibt es vier Grundarten von Identitätsmanagementsysteme in Anwendungen:

- Isolierte Identitäten, z.B. in einem Unternehmen
- Zentrale Identität; z.B. ein Account, zur Anmeldung bei unterschiedlichen Services (vgl. Ziff. 1.7.1 und Ziff. 3.7.1)
- Föderierte Identitäten; z.B. die eIDAS-Identitäten im EU-Raum mit seinen Mitgliedsstaaten
- Dezentrale Identität (englisch Decentralized Identity, abgekürzt DID); z.B. Self Sovereign Identity (SSI)

Mit der eIDAS-Verordnung werden vier Grundfunktionen bei den föderierten Identitäten im EU -Wirtschaftsraum unterschieden:

- Identitätsprovider (IDP), der die Identitäten von Personen überprüft;
- Serviceprovider (SP), der einen Dienst oder mehrere Dienste anbietet;
- Attribute-Provider (AP), der bestimmte Attribute einer Identität herausgibt, um eine Prüfung durchzuführen; z.B. die Person ist mindestens 18 Jahre alt.
- eIDAS Knoten Betreiber (eIDAS node operator), der in jedem Mitgliedsland der Verbindungsknoten (Konnektor) zu den anderen Mitgliedsländern ist

Bei einem isolierten Identitätsmanagementsystem fallen die Grund-Funktionen des IDP, SP und AP in einer einzigen Firma (privat) oder Einrichtung (öffentlich) zusammen. In einem zentralen Identitätsmanagementsystem fallen IDP und AP zusammen. Es können jedoch mehrere, nicht dem IDP/AP organisatorisch zugeordnete SPs bedient werden.

Werden Identitäten föderiert verwaltet, so werden diese Funktionen von nicht zusammengehörigen Organisationen bereitgestellt, welche jedoch über ein entsprechend geregeltes Vertrauensverhältnis den gegenseitigen Datenaustausch erlauben bzw. ermöglichen. Das eIDAS-Rahmenwerk spezifiziert ein föderiertes Identitätsmanagement-System. Kernelement ist hier der eIDAS-Knoten, welcher den grenzüberschreitenden Datenaustausch zwischen IDP, AP und SP technisch umsetzt. Auch dem Onlinezugangsgesetz liegen föderierte Identitätsmittel zugrunde, indem von jedem Verwaltungsportal aus jede beliebige Verwaltungsleistung genutzt werden kann.

Beispiel eines zentralen Identitätsmanagementsystems: *Student X verfügt über ein Benutzerkonto, das zur Authentifizierung von unterschiedlichen (Online-)Diensten der Universität genutzt wird. Damit fallen IDP und AP in einer Einrichtung zusammen.*

3.3

Datenschutz bei Identifikationssystemen

Vergleicht man die analoge mit der digitalen Welt, so wird mit dem Identitätsprovider eine neue „Rolle“ definiert, die es in der analogen Welt nicht gab. Es bestehen dazu heute unterschiedliche Ausprägungen in Deutschland, wie das Post-Ident- und das Video-Ident-Verfahren sowie die Dienste des Bundesverwaltungsamts (BVA), das Berechtigungszertifikate nach einer elektronischen Identitätsüberprüfung erstellt und an Wirtschaftsunternehmen und Verwaltungsbehörden ausgibt. Diese erhalten nur dann Zugang zu den elektronischen Ausweisdaten des Personalausweis-Inhabers, wenn sie erfolgreich eine Berechtigung bei der Vergabestelle für Berechtigungszertifikate des BVA beantragt haben.
Im Kontext der Identitätsüberprüfungen wird auch der Begriff KYC (Know Your Customer) zunehmend verwendet, welcher einen erhöhten Mindeststandard zur Identifikation von Personen bzw. Kunden vorsieht.

Beispiel für eine KYC-Ansatz: *Die Kontoeröffnung nach § 11 GwG ist mit dem Video-Ident Verfahren zugelassen. Dazu wird der Ausweis für die Kamera eines PCs oder Tablet so lange bewegt, bis die optischen Sicherheitsmerkmale mit einem KI-Algorithmus und den ausgewerteten Kamerabildern hinreichend verifiziert worden sind.*

Videoidentifizierungsverfahren sind jedoch aufgrund bestehender Manipulationsmöglichkeiten nicht für alle Einsatzzwecke geeignet, insbesondere solche, bei deinen ein sehr hohes Vertrauensniveau bestehen muss.

Werden personenbezogene Daten verarbeitet, ist strikt auf die Einhaltung der datenschutzrechtlichen Vorgaben zu achten. Datenschutzkritisch kann der IDP-Ansatz dann werden, wenn der Identitätsprovider die genutzten Online-Dienste elektronisch speichert und daraus ein „Profil“ entwickelt wird, inklusive individuellen Online-Nutzungsinformationen, mit Datum und Zeit. Wird der gesamte Prozess zunehmend automatisiert, besteht die Gefahr, dass der Bürger keine Transparenz darüber besitzt, wann, an wen und zu welchem Zweck seine persönlichen Daten weitergegeben wurden. Auch an dieser Stelle können PIMS einen wichtigen Beitrag dazu leisten, solche Datenströme für den Nutzer transparent aufzubereiten und damit beherrschbar zu machen. Dies wäre etwa denkbar im Rahmen von Dashboards und integrierten Aktivitätsverläufen.

3.4

Technologien für Identitäten und abgeleitete Identitäten

Zur Erteilung eines Ausweises als hoheitliches Dokument, der die Identität einer Person bestätigt, ist nach deutschem Recht ein gültiges oder abgelaufenes Identitätsdokument (Pass oder Personalausweis) sowie ein biometrisches Lichtbild vorzulegen. In bestimmten Fällen können zusätzlich Geburts- oder Abstammungsurkunden erforderlich werden. Danach werden die Daten durch die Meldebehörde an die Bundesdruckerei übermittelt, die in sicherer Umgebung ein neues Identitätsdokument herstellt, welches an den Bürger übergeben wird.
Auch Mobiltelefone eignen sich als Trägermedium von Identitätsdaten. Werden Identitätsdaten bzw. persönliche Attribute aus dem Personalausweis auf ein Smartphone übertragen und zum Beispiel in einem Chip gespeichert, spricht man von abgeleiteten Identitäten.

Beispiel für abgeleitete Identitäten: *Im Projekt OPTIMOS 2 wird eine technische Umsetzung mit bestehenden Standards, wie Near Field Communication (NFC) und bekannten Komponenten, wie der elektronische Personalausweis und NFC-fähigen Smart Phones in verschiedenen Anwendungen getestet, bei denen auch die abgeleitete Identität zum Einsatz kommt*[34].

[34] https://www.ausweisapp.bund.de/fileadmin/user_upload/Anwenderforen/190121-Optimos2%40AusweisApp2Forum-as_sent.pdf

3.5

Umsetzungsmöglichkeiten von Identifikationssystemen

Die eIDAS-Verordnung unterscheidet zwischen

- Identifikationsmitteln und
- Identifikationssystemen

Zu der Klasse der Identifikationsmittel zählen der elektronische Personalausweis, das Smartphone mit Sicherheitselement (abgeleitete Identität), aber auch FIDO-Token (Fast Identity Online; zur passwortlosen Authentifizierung), also jene Komponenten, welche zur sicheren Identifizierung und Authentifizierung an einem Identifikationssystem verwendet werden. In der Praxis weit verbreitet sind im Übrigen Identifizierungen mittels einseitiger Erklärungen der Nutzer (self-declaration), so beispielsweise, wenn sich Nutzer mit einem Double-Opt-In bei einem Webseitendienst anmelden.
Identifikationssysteme (IDPs) im Kontext der eIDAS-Verordnung können unterschiedlich umgesetzt werden. Als Identifikationssystem können zentrale Registrierungssysteme verwendet werden, bei denen z.B. das jeweils gewählte Identifikationsmittel, wie ein FIDO-Token, einmalig erfasst wird. Gemäß der eIDAS klassifizierte Identifikationssysteme können jedoch auch Authentifizierungsdienste wie das Bundesverwaltungsamt (BVA), oder private Diensteanbieter zur Identifikation sein.
Neben den IDPs bestehen andere Modelle der „selbstbestimmten Identität". Darunter fallen Technologien wie die Self Sovereign Identity (SSI), die wahlweise in Verbindung mit Blockchain, konkreter mit der Distributed Ledger Technologie (DLT) genutzt werden. Sie basieren auf internationalen Standards, wie W3C mit dem Konzept Verifiable Credentials (VC), in denen technologische Aspekte rund um authentische Attribute beschrieben werden und stellen die Klasse der verteilten bzw. dezentralen Identitätsmanagementsysteme dar. Ein SSI System selbst bietet dabei typischerweise keine Identifizierungsmittel an, sondern liefert nur den Dienst, den der Nutzer hierfür verwenden will.

Beispiel für eine SSI-Lösung in der Praxis: *Um Ausbildungsbescheinigungen fälschungssicherer zu machen, wird ein VC-basiertes Zertifikat an den Teilnehmer ausgestellt, an sein Smartphone gesendet und in der SSI-Wallet gespeichert. Die Firma oder Ausbildungsstelle, die die Bescheinigung ausgestellt hat, sendet einen QR-Code auf eine E-Mail-Adresse der Person. Dieser QR-Code wird mit dem Smartphone eingescannt und der Inhaber des Smartphones erhält ein Zertifikat. Gleichzeitig wird mit der Annahme eine Meldung zur Entgegennahme zurückgesandt. (Quelle: BITKOM[35])*

[35] https://www.bitkom.org/Bitkom/Publikationen/Self-Sovereign-Identity-Use-Cases.

3.6

Branchenspezifische Ausgestaltung der Identitätsnachweisqualitäten

Bereits die eIDAS-Verordnung zeigt auf, dass es eine Vielzahl unterschiedlicher Einsatzszenarien mit unterschiedlichen Anforderungen an die Verlässlichkeit der Identität gibt. Auch in Zukunft wird es Identitätsmanagementsysteme geben, die Identitätsnachweise in nicht gesetzlich vorgeschriebenen oder näher geregelten Fällen sicherstellen werden. Diese Optionen sollten auch beibehalten werden. Gerade soweit die von der eIDAS-Verordnung vorgesehenen Nachweisstufen entweder zu hohe oder zu niedrige Garantien bieten, sollte es Branchen ermöglicht sein, ergänzende, auf die speziellen Bedürfnisse ausgerichtete Nachweise zu etablieren. Hierbei sollten auch Szenarien berücksichtigt werden, die abseits der in der eIDAS-Verordnung geregelten hohen Vertrauensstufen existieren, so im Bereich der bereits erwähnten „self-declaration“ der Nutzer.

3.7

Praxisbeispiele

3.7.1 Single-Sign-On

3.7.1.1 Einsatzzwecke/Szenarien

Single Sign-On (SSO) stellt ein Authentifizierungsverfahren dar, das Anwender auf Grundlage eines einzi-gen Authentifizierungsprozesses (also mit nur einem Nutzeraccount) Zugriff auf mehrere unterschiedliche Dienste ermöglicht. Der SSO-Dienst hat somit die Aufgabe, die Nutzer-Identität gegenüber den beteiligten Diensten zu bestätigen und die Authentifizierung vorzunehmen. Typischerweise verwaltet der SSO-Dienst zusätzlich auch Stammdaten von Nutzern und ermöglicht es Diensten, die Weitergabe dieser bei Nutzern anzufragen, d.h. die Autorisierung der Weitergabe von personenbezogenen Daten zu steuern und zu verwalten. Der SSO-Dienst erlaubt somit die Nutzung verschiedener Dienste mit nur einem Account, über den sich Nutzer gegenüber Diensten authentifizieren können und die Weitergabe von Stammdaten an den Dienst steuern. Eine separate Registrierung bei jedem dieser Dienste kann somit entfallen bzw. wesentlich vereinfacht werden.

Es existieren unterschiedliche Arten von SSO-Diensten und auch verschiedene Einsatzgebiete. In der vorliegenden Betrachtung stehen SSO-Dienste im Mittelpunkt, die Endnutzern den Zugriff auf unterschiedliche Online-Dienste ermöglichen. Verbreitete Beispiele hierfür sind sog. „Social Logins“ oder auch „e-Commerce-Logins“ großer Online-Plattformen. Diese Dienste bieten, neben der Funktion „Login“, typischerweise auch zusätzliche Dienste an, die mit dem Login korrespondieren. Ein Beispiel hierfür sind E-Commerce-Logins, die gleichzeitig auch Zahlungsinformationen und -vorgänge anbieten. Ein weiterer im Besonderen im Kontext Datenschutz relevanter Aspekt wäre die Funktion als Einwilligungstreuhänder als zusätzliche Funktion eines SSO-Dienstes. Darüber hinaus kommen SSO-Prozesse beispielsweise auch im Kontext von Unternehmens-IT oder akademischen Umfeld zum Einsatz, um den Zugriff auf unterschiedliche Unternehmens-Applikationen zu ermöglichen (Enterprise SSO).

Auf technischer Ebene existieren verschiedene Standards, mit denen sich SSO-Verfahren realisieren lassen. Bei webbasierten Diensten ist insbesondere OpenID Connect als Authentifizierungs-/Autorisierungsprotokoll zu nennen, das weit verbreitet ist und weltweit genutzt wird, im Besonderen im B2C-Bereich. Wichtig ist dabei, dass es sich um technische Protokolle handelt, die keine datenschutzrechtlichen Komponenten und Einordnungen aufweisen oder vornehmen. Der datenschutzkonforme Einsatz von SSO-Diensten hängt ausschließlich von ihrer Implementierung ab (vgl. Ziff. 3.7.1.3) und unterscheidet sich bei den aktuell im Markt verfügbaren Diensten deutlich.

3.7.1.2 Chancen und Risiken

SSO-Dienste bieten Nutzern eine Reihe an Vorteilen gegenüber mehreren individuellen Authentifizierungen und Registrierungen bei den genutzten Diensten.

- An erster Stelle ist dabei die hohe Nutzerfreundlichkeit zu nennen: Anstatt für jeden Dienst eigenständige Anmeldeinformationen anzulegen, ermöglichen SSO-Dienste eine Zeitersparnis, weil nicht immer wieder neue Log-in-Informationen eingegeben werden müssen.
- Dadurch erhöht sich auch die Sicherheit: Phänomene wie die Mehrfachverwendung von Passwörtern können durch den Einsatz von

SSO-Diensten reduziert werden. Nutzer benötigen nur noch ein Login für den Zugriff auf unterschiedliche Dienste. Auch die Gefahr von Phishing-Angriffen wird durch die Reduktion auf eine Stelle vermindert.

- Für Nutzer entsteht zudem ein spürbarer Vorteil hinsichtlich der Transparenz und Kontrollmöglichkeiten: Der SSO-Dienst kann die Rolle eines Treuhänders einnehmen, der eine transparente Übersicht bietet, wo Login-Daten genutzt werden. Nutzer können auf diesem Weg Kontrolle über ihre Daten ausüben und jederzeit die Datenweiterleitung bei der Nutzung einzelner Dienste beenden. Eine solche Form der Transparenz und Übersicht darüber, welche Dienste über welche Daten verfügen, ist bei einer Vielzahl individueller Logins kaum vorstellbar.
- Bei der Nutzung eines SSO-Dienstes kommt noch der Vorteil der automatischen Aktualisierung von Stammdaten hinzu. Beispielsweise können über einen SSO-Dienst Änderungen an der Postanschrift an zentraler Stelle vorgenommen werden, die sich dann in angeschlossenen Diensten (wie beispielsweise dem Zeitungsverlag) automatisch aktualisieren.

Die hohe Nutzerfreundlichkeit des diensteübergreifenden Zugriffs birgt jedoch auch das Risiko des „Identitäts-Diebstahls“: Der Übernahme einer SSO-Identität könnte einen Zugriff auf gleich mehrere der angeschlossenen Dienste möglich werden. Auch der Ausfall eines SSO-Dienstes kann für Nutzer bedeuten, dass auf angeschlossene externe Dienste nicht mehr zugegriffen werden kann. Dies kann auch im Falle von Accountsperren (z.B. infolge von fehlerhaften Passworteingaben) eintreten. Ebenso bedarf das Risiko einer über die eigentliche Zweckbestimmung des SSO-Dienstes hinausgehenden Datennutzung besonderer Beachtung. So sind bspw. Auswertungen eines Nutzerverhaltens zu Werbezwecken transparent zu beschreiben und mit einer Einwilligung der Betroffenen zu begleiten. Gleiches gilt für eine diensteübergreifende Profilierung des Nutzerverhaltens durch WerbeIDs (vgl. nachfolgend Ziff. 3.7.2).

3.7.1.3 Anforderungen

SSO-Dienste können Komfort und Nutzerfreundlichkeit von Online-Diensten enorm erhöhen. Gleichzeitig besteht ein Missbrauchs- und Datenschutzrisiko, da mit unterschiedlichen persönlichen Login-Informationen an einer zentralen Stelle gearbeitet wird. Wie eingangs erläutert, regulieren die existierenden SSO-Standards keine datenschutzrechtlichen Fragen. Aus diesem Grund ist es zwingend erforderlich, dass für Nutzer Klarheit hinsichtlich der SSO-Funktion und der Funktionsweise besteht.

Die folgenden Aspekte sollten SSO-Dienste auf jeden Fall berücksichtigen, um Nutzern eine souveräne Nutzung zu ermöglichen:

- Es muss klar erkennbar sein, welche genaue Rolle der Dienst einnimmt. Die Authentifizierung/Autorisierung für einen Dienst ist die Kernfunktionalität des SSO-Dienstes. Es muss für Nutzer jedoch jederzeit transparent ersichtlich sein, welche ggf. darüberhinausgehende Rolle der SSO-Dienst einnimmt. Es ist beispielsweise denkbar, dass über die Datenübermittlung zur Erbringung des SSO-Dienstes hinaus weitere Verarbeitungen zu werblichen Zwecken durch den SSO-Dienst selbst vorgenommen werden. Verarbeitungstatbestände, die Nutzer nicht mit dem SSO-Dienst assoziieren, müssen transparent sein, damit eine bewusste Nutzungsentscheidung und Verarbeitungseinwilligung getroffen werden kann. Für Dienste, die auf den SSO zurückgreifen, ist dies natürlich

ebenfalls von hohem Interesse.

- Beim Einsatz von Logins muss es für Nutzer erkenntlich sein, wenn es sich um ein SSO-Login handelt. Es darf nicht die Situation entstehen, dass ein vermeintlich individuelles Login eines Dienstes Auswirkungen auf benachbarte Dienste hat, ohne dass dies für Nutzer ersichtlich wird und diese dies aktiv steuern können.
- Hiermit verwandt ist die Frage nach der Transparenz zum Login-Status. Nutzer müssen jederzeit die Kontrolle und Transparenz über ihren Anmeldestatus haben. Dies erfordert allerdings das Zusammenspiel von SSO-Dienst und verknüpftem Dienst, bei dem Nutzer angemeldet sind, und ist nicht allein durch den SSO-Dienst adressierbar.

3.7.2 Advertising Identities

3.7.2.1 Rechtliche und technische Einordnung

Digitale Identitäten erlauben die Personalisierung von Produkten und Dienstleistungen im Internet. Die Nutzung im Advertising-Bereich ist daher nur ein möglicher Einsatzzweck neben vielen anderen kommerziellen Geschäftsmodellen. Hierbei sei erwähnt, dass in Abhängigkeit von Gerät (Desktop-PC, Smartphone, Smart-TV, ...) und Umgebung (Web oder App) vielfältige technische Ausprägungen der digitalen Identitäten respektive deren Speicherung bestehen. Typischerweise assoziiert eine Advertising Identity technische Rahmendaten des Nutzers (Browser, Betriebssystem, Endgerät, etc.), soziodemographische Merkmale (Alter, Geschlecht, Hausstand) sowie Interessen und Intentionen z.B. basierend auf seinem Surfverhalten. Damit sind sie personenbezogen oder zumindest personenbeziehbar bzw. pseudonym, da sie zur Identifizierung einer natürlichen Person genutzt werden können. Sie unterliegen deshalb der DS-GVO (Art. 4 Abs. 1 DS-GVO). Für den Aufbau und die Nutzung von Identitäten ist deshalb eine rechtliche Grundlage erforderlich, die häufig ein Vertrag mit der betreffenden Person (Art. 6 Abs. 1 lit. b DS-GVO) oder eine Einwilligung der betreffenden Person (Art. 6 Abs. 1 lit. a DS-GVO) umfasst. Es sind aber auch andere rechtliche Grundlagen möglich, wie z.B. für ein Reichweiten-Tracking.

Wurden im Web(-Browser) Identitäten typischerweise in sog. Cookies vorgehalten, so stellen mobile Betriebssysteme (iOS, Android) für App-Umgebungen eine pseudonyme Identität bereits in deren Betriebssystem zur Verfügung. Auch geräteübergreifende Identitäten sind möglich, insbesondere dann, wenn diese serverseitig vorgehalten und z.B. durch einen Login-Vorgang dem User zugeordnet werden können. Eine solche übergreifende pseudonyme Identität kann auch mit einem SSO-Dienst angeboten werden.

Neben der Identität selbst, die meist nicht der direkten Identifikation, sondern vielmehr einer pseudonymen Personalisierung dient, sind mit dieser Identität assoziierte Daten von zentraler Bedeutung. Die Effizienz einer zielgerichteten Werbeaussteuerung steht in Abhängigkeit von mit der Identität assoziierbaren Daten. Beim sog. Programmatic Advertising werden mittels eines technisch automatisierten Einkaufs- und Werbeauslieferungsprozesses Daten zur Anwendung gebracht, die vormals nur schwerlich für die Werbung aktivierbar waren. Hierbei gelten besondere Anforderungen an die Transparenz der Verarbeitung sowie ihre Rechtmäßigkeit mittels einer Einwilligungserklärung.

Marktstandards wie der des IAB Europe Transparency & Consent Frameworks (TCF) erlauben es

[36] RTB oder Real-Time-Advertising beschreibt nur einen Bestandteil des Programmatic Advertising. Konkret den Teil, bei dem Media in einem Auktionsprozess versteigert und daraufhin Werbung automatisiert aus-geliefert wird.

Internetnutzern, die beteiligten Parteien an der Werbeauslieferung nachzuvollziehen und auch auf deren Einsatz einzuwirken (Einwilligung, Opt-Out, etc.). Sie stellen damit Funktionalitäten eines PIMS bereit.

3.7.2.2 Herausforderungen und Lösungsansätze

Die digitale Wirtschaft wird nicht nur von staatlicher Seite reglementiert, sondern ist zunehmend dem „Gatekeeping“ seitens der Browser (Chrome, Firefox, Safari, Edge) und Betriebssysteme (Android, iOS, Windows) meist aus dem außereuropäischen Raum ausgesetzt.

Eine europäisch getragene digitale Identität sowohl für die Werbewirtschaft als auch für Diensteanbieter im Internet kann eine dauerhafte Vielfalt im „freien Internet“ außerhalb der marktdominanten Plattformen ermöglichen. Für eine informierte Einwilligung der Nutzer in die Erzeugung und Nutzung einer solchen Identität, wäre insbesondere Transparenz herzustellen über Rollen und Funktionen von Anbietern solcher Identitäten. Ferner sind dem Nutzer Transparenz und Steuerungsmöglichkeiten über seine personenbezogenen Daten, welche mit digitalen Identitäten verknüpft werden, einzuräumen. Hierbei ist die Schaffung gemeinsamer Standards auf internationaler Ebene denkbar.