Smart Data

Sicheres Identitätsmanagement im Internet

Eine Analyse des ISÆN-Konzepts (Individual perSonal data Auditable addrEss) durch die Smart-Data-Begleitforschung im Auftrag des Bundesministeriums für Wirtschaft und Energie

Impressum

Herausgeber
Smart-Data-Begleitforschung
FZI Forschungszentrum Informatik
Außenstelle Berlin
Friedrichstr. 60, 10117 Berlin
www.smart-data-programm.de

Beteiligte Partner der Analyse
FZI Forschungszentrum Informatik
Fraunhofer IESE
ITSO GmbH
BBW-Hochschule
und Peter Schaar, Vorsitzender der Europäischen
Akademie für Informationsfreiheit und Datenschutz

Gestaltung
LoeschHundLiepold Kommunikation GmbH, Berlin

Stand
März 2017

Druck
WIRmachenDRUCK GmbH

Bildnachweis
agsandrew – Fotolia.com (Titel)
KIT (S. 53, Quade)
peter-schaar.de (S. 56, Schaar)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

1 Zusammenfassung

Die französische Standardisierungsinitiative ISÆN (Individual perSonal data Auditable addrEss Number) beschreibt ein Konzept, das es Bürgern bei der Nutzung von Internet-Dienstleistungen ermöglichen soll, die Kontrolle über ihre personenbezogenen Daten zu behalten. Die Datenschutzprinzipien „Transparenz“ und „Nachvollziehbarkeit“ sollen hierbei durch technische Maßnahmen gestärkt werden. Mit ISÆN sollen betroffene Personen jederzeit nachvollziehen können, wer welche ihrer personenbezogenen Daten verarbeiten darf. Darüber hinaus sollen sie diese Rechte jederzeit einschränken können. Eine Weitergabe personenbezogener Daten findet nur dann statt, wenn die betroffenen Personen eingewilligt haben. [1]

Technologie

Technologisch sieht das ISÆN-Konzept die Einführung eines eindeutigen Bezeichners (des ISÆN-Identifiers), eines Blockchain-Netzwerks sowie Anwendungen für Personen (Benutzer), beispielsweise per Smartphone-App, vor. In der Blockchain sollen Repräsentationen von Datenschutzeinwilligungen manipulationssicher, transparent und nachvollziehbar gespeichert werden. Die individuellen personenbezogenen Daten sollen – z. B. durch biometrische Verfahren geschützt – in der jeweiligen Anwendung der Benutzer gespeichert und durch diese erst, nachdem die Person eine Autorisierung erteilt hat, an Dienstleister übertragen werden.

Bewertung

Die auf Basis von ISÆN angedachte Unterstützung zur Umsetzung von Datenschutzgrundsätzen mittels technischer Maßnahmen stellt einen vielversprechenden Ansatz dar. Die Verwendung eines einsehbaren, manipulationssicheren Speichers kann sowohl für Dienstanbieter im Hinblick auf entsprechende Dokumentations- und Informationspflichten hilfreich sein, als auch für Personen, um jederzeit Erkundigungen über Zugriffe auf ihre personenbezogenen Daten einholen zu können.

Die im ISÆN-Konzept zum Einsatz kommende Blockchain-Technologie stellt ebenso einen vielversprechenden Ansatz zur nachvollziehbaren und sicheren Aufzeichnung der Datenbewegungen von Benutzern dar. Insbesondere die für eine datenschutzkonforme Ausgestaltung bzw. Umsetzung notwendigen Implementierungsentscheidungen sollten in Folgeprojekten (insbesondere mit den französischen Partnern) untersucht werden.

ISÆN kann das Potenzial besitzen, der elektronischen Identifizierung und dem Anbieten von Vertrauensdiensten für elektronische Transaktionen im EU-Binnenmarkt zu einem Durchbruch zu verhelfen. Grundsätzlich ist es wünschenswert, die Verwendung von Identifizierungssystemen auch im Privatsektor weiter voranzutreiben, insbesondere um das Vertrauen in den elektronischen Geschäftsverkehr zu stärken. Potenziell entstehende Zielkonflikte, die sich insbesondere auch aus rechtlicher Sicht ergeben können, müssen anhand der Betrachtung konkreter Anwendungsfälle aufgelöst werden.

2 Ausgangslage und Motivation

Eine Grundlage unserer heutigen Wissensgesellschaft sind die Nutzung und der Austausch von Information. Daten, aus denen diese Information gewonnen werden kann, werden als das „neue Öl“ bezeichnet, das Wirtschaftszweige antreiben kann. Der Austausch personenbezogener Daten ist dabei jedoch zukünftig nur im Rahmen der neuen europäischen Datenschutz-Grundverordnung (DSGVO) zulässig. Diese fordert insbesondere:

- die Festlegung der Verarbeitungszwecke,
- das Einholen einer klar und verständlich formulierten Einwilligung der betroffenen Personen, soweit die Verarbeitung ohne gesetzliche Ermächtigung erfolgt,
- ein Widerspruchsrecht der betroffenen Personen bezüglich der Verarbeitung ihrer Daten,
- die Informationspflicht und das Recht der betroffenen Personen auf Auskunft über gespeicherte oder übermittelte personenbezogene Daten,
- die Informationspflicht bei der Weitergabe personenbezogener Daten,
- ein Recht auf Datenlöschung, soweit die Voraussetzungen für die Datenverarbeitung nicht bzw. nicht mehr bestehen („Recht auf Vergessenwerden“),
- das Verbot automatisierter Einzelentscheidungen zu Lasten der betroffenen Person.

Die französische Standardisierungsinitiative ISÆN verfolgt das Ziel, sowohl Bürgern als auch Unternehmen einen möglichst sicheren Umgang mit personenbezogenen Daten zu ermöglichen und so die Grundrechte der Bürger bei der Verarbeitung von digitalen Daten zu stärken. ISÆN beschreibt, wie in einem sicheren Metaregister Angaben über die Speicherung und Weitergabe personenbezogener Daten unter Beachtung der DSGVO erfasst werden. Die betroffenen Personen können jederzeit einsehen, wer Daten über sie in welchem Umfang speichert, und über Opt-in-/Opt-out-Mechanismen ihre Zustimmung geben oder diese auch wieder entziehen.

In der vorliegenden Studie soll das Potenzial von ISÆN bewertet werden, um in einem nächsten Schritt – z. B. in einem deutsch-französischen Projekt, möglichst sogar mit weiteren europäischen Partnern – Technologien zu entwickeln, die die europäischen Anforderungen und Datenschutzvorgaben umsetzen. Dieses Projekt kann ein wichtiger Schritt zur Umsetzung der aus der eIDAS-Verordnung resultierenden Anforderungen hinsichtlich der elektronischen Identifizierung und des Anbietens von Vertrauensdiensten für elektronische Transaktionen im EU-Binnenmarkt werden. Durch die bilaterale Zusammenarbeit und die frühzeitige Einbindung von (mittelständischen) Partnern aus der Wirtschaft kann eine hohe Akzeptanz der zu entwickelnden Technologien erreicht werden.

3 ISÆN – Individual perSonal data Auditable addrEss Number

Die französische Standardisierungsinitiative ISÆN verfolgt das Ziel, sowohl Bürgern als auch Unternehmen einen möglichst sicheren Umgang mit personenbezogenen Daten zu ermöglichen und so den Schutz personenbezogener Daten der Bürger bei der Verarbeitung und Nutzung von Daten zu stärken.

In der vorliegenden Studie wird der Begriff ISÆN sowohl für die Standardisierungsinitiative selbst als auch für konkrete Umsetzungen und damit einhergehende Technologien verwendet.

3.1 Typischer Anwendungsfall

Beim Einkauf in einem Webshop werden zur Abwicklung des Kaufs üblicherweise Angaben zur Person (Name, Vorname, Liefer- und Rechnungsadresse) und zur Abrechnung, beispielsweise Kreditkarten-Daten des Käufers, vom Händler erfasst. Vom Käufer muss dabei unter Umständen eine Einwilligung in die Nutzung und Verarbeitung seiner personenbezogenen Daten eingeholt werden (Datenschutzerklärung).

Durch den Einsatz einer Technologie, wie sie die ISÆN-Initiative vorschlägt, sollen das Erfassen der personenbezogenen Daten bei der Abwicklung solcher Transaktionen und deren weitere Speicherung transparenter und auch sicherer werden.

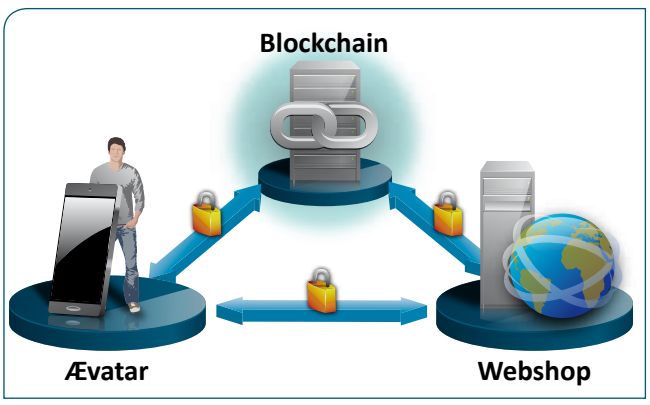

Abbildung 1: schematische Darstellung der Datenflüsse im Anwendungsszenario

Eine Implementierung von ISÆN besteht im Wesentlichen aus einer Anwendung (einer „virtuellen Brieftasche“, in unserer Studie die App „Ævatar“) für ein Smartphone, in der die persönlichen Daten des Nutzers abgesichert, beispielsweise durch biometrische Zugangsverfahren wie Fingerprint oder Gesichtserkennung, gespeichert werden, während in einem so genannten Blockchain-Netzwerk die Transaktionen (Zugriffe und Informationen über die eventuelle Weitergabe der Daten) protokolliert werden. Die Blockchain enthält dabei nur die Beschreibung der Transaktionen (Transaktions- bzw. Metadaten), niemals aber die Daten selbst. Der Datenaustausch zwischen dem Nutzer und dem Internet-Dienstanbieter (hier: Webshop) erfolgt erst nach Freigabe durch den Nutzer direkt und ist ebenso verschlüsselt wie die Kommunikation mit dem Blockchain-Netzwerk. Wir beschreiben im Folgenden die wesentlichen Schritte der Verwendung des Verfahrens, die Registrierung als Nutzer des Verfahrens und die Verwendung am Beispiel eines Kaufs bei einem Online-Händler.

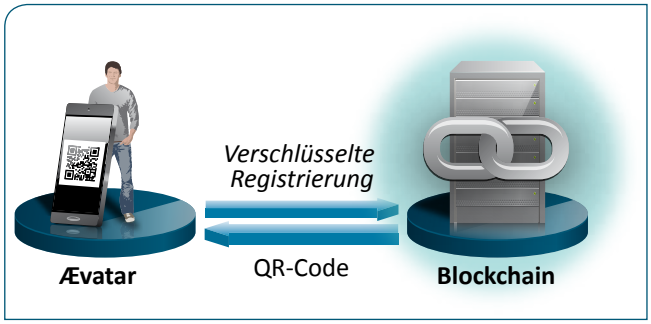

Abbildung 2: Registrierung in der Blockchain

Wir gehen davon aus, dass sich die Ævatar- App auf dem Smartphone befindet. Der Nutzer registriert sich bei dieser durch Angabe seiner persönlichen Daten. Aus diesen Daten wird ein Hashwert gebildet, ein neuer Account in der Blockchain eingerichtet und der Hash dort gespeichert.

Dieser Hashwert dient im Folgenden zur eindeutigen Identifikation (ID) des Benutzers und wird auf dem

Smartphone auch als QR-Code gespeichert. Der QR-Code kann in der Folge anstelle des (länglichen) Hashwerts bei einer Anfrage der Daten verwendet werden.

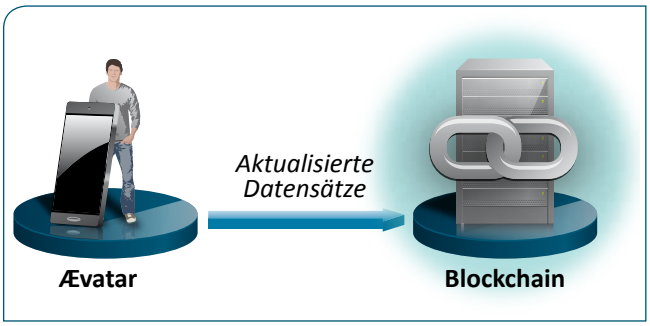

Abbildung 3: Aktualisierung der persönlichen Daten

Der Nutzer kann seine persönlichen Daten in Ævatar jederzeit aktualisieren. Diese Aktualisierung führt dann zu einem weiteren Eintrag in der Blockchain. Dabei wird wiederum nur übertragen, welche Daten geändert wurden, nicht aber die tatsächlichen Werte (beispielsweise führt eine Änderung der Anschrift in der Blockchain nur zu einem Eintrag „Anschrift geändert“). Alle Systeme, die persönliche Daten des Nutzers über die oben beschriebenen Mechanismen speichern und verarbeiten, sollen damit erkennen können, dass die von ihnen verwendeten Daten nicht mehr aktuell sind.

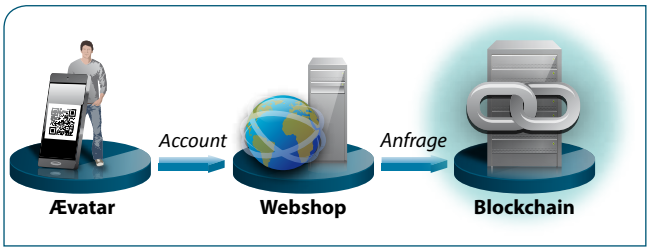

Abbildung 4: Persönliche Daten des Nutzers werden per QR-Code übertragen

Möchte ein Internet-Dienstanbieter (beispielsweise der Betreiber eines Webshops) auf die Daten des Anwenders zugreifen, kann der Anwender den QR-Code (grafische Darstellung seines Hashs) z. B. mit seinem Smartphone vor die Kamera eines Laptops oder eines geeigneten Barcode-Scanners halten und so dem Dienstanbieter seine ID in der Blockchain übermitteln.

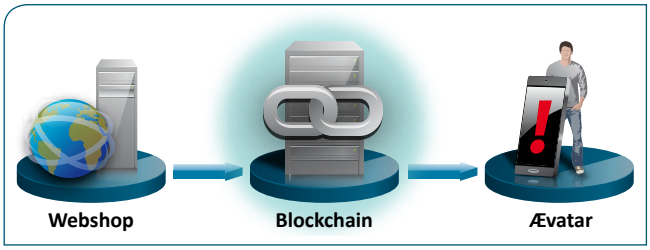

Abbildung 5: Anfrage persönlicher Daten

Über die Blockchain soll anschließend eine Anfrage an das Smartphone des Anwenders bzw. an die Ævatar-App gerichtet werden, ob der Internet-Händler auf Daten, wie beispielsweise Name und Vorname, zugreifen darf. Auch diese Anfrage wird in der Blockchain protokolliert.

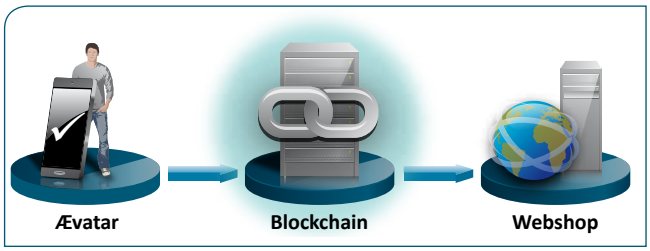

Abbildung 6: Anwender erteilt Zustimmung

Die Anfrage wird dem Anwender auf dem Mobiltelefon angezeigt, woraufhin er seine Zustimmung geben oder diese verweigern kann. Die Zustimmung oder Verweigerung hinsichtlich der Datennutzung wird wiederum in der Blockchain protokolliert.

Bei Zustimmung erfolgt dann die Übertragung der angeforderten Daten direkt zwischen Anwender und Dienstanbieter mit üblichen, dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Mit den in der Blockchain gespeicherten Informationen soll der Nutzer jederzeit die Möglichkeit haben, nachzuvollziehen, wem er welche Autorisierung zur Verwendung seiner personenbezogenen Daten gegeben hat.

3.2 Ergänzungen zum Anwendungsfall

3.2.1 Teilnehmer des ISÆN-Blockchain-Netzwerks

Benutzt eine Anwendung eine eigene Blockchain, stellt sich die Frage nach den Teilnehmern des Blockchain-Netzwerks. Entsprechende Anreize vorausgesetzt, könnten die Knoten der ISÆN-Blockchain, d. h. die Rechner, auf denen die verteilte Blockchain gespeichert ist und auf denen neue Blöcke errechnet werden, beispielsweise durch die teilnehmenden Organisationen und Unternehmen bereitgestellt werden.

3.2.2 Szenarien für die Weitergabe von personenbezogenen Daten

Die Weitergabe von personenbezogenen Daten ist nicht auf das oben beschriebene Szenario beschränkt. Der Einsatz eines Systems wie ISÆN ist vielmehr in unterschiedlichen Szenarien denkbar. Beispielsweise kann auch eine sichere und nachvollziehbare Weitergabe von Daten, die in einem Unternehmen X über eine Person Z gespeichert sind und an eine Organisation Y weitergegeben werden sollen, realisiert werden, sofern X und Y ISÆN unterstützen.

Beispiel: Die Person Z verwendet Dienste des Unternehmens X, um auf den Servern von X eigene Fotos zu speichern. X möchte nun im Rahmen einer Werbekampagne einzelne Fotos der Person Z an die Organisation Y senden. Dazu wird eine Anfrage an Z gesendet, ob Z dieser Weitergabe zustimmt (Anfrage wird in der Blockchain gespeichert). Z erteilt seine Zustimmung (Zustimmung wird in der Blockchain gespeichert) und anschließend sendet X die genehmigten Fotos an Y (die Information über diese Transaktion wird ebenfalls in der Blockchain gespeichert) über eine abgesicherte Verbindung.

Die Übertragung komplexer Datenstrukturen ist ebenso möglich (siehe hierzu beispielsweise OASIS XDI[2]).

3.3 Grundlegende Anforderungen an einen Identifier

Aus technischer Sicht gibt es unterschiedliche Anforderungen an Identifier, die je nach Anwendungsfall notwendig sind:

- aussagekräftig für Menschen: Der Identifier soll für Benutzer verständlich sein.
- aussagekräftig für Maschinen: Der Identifier soll maschinenlesbar sein.
- dezentralisiert: Zwischen ausstellenden Instanzen gibt es keine horizontalen Vertrauensbeziehungen. Es gibt keine zentrale Autorität.
- sicher: Die Integrität des Identifiers ist gewährleistet. Niemand kann die Zuordnung unbemerkt manipulieren.

Laut der Theorie „Zookos Dreieck“ können in einem Namensraum nicht gleichzeitig die Eigenschaften „Aussagekräftig“, „Dezentralisiert“ und „Sicher“ erfüllt werden, sondern jeweils nur zwei dieser Eigenschaften.

ISÆN will dieses Problem lösen, indem aus dem aussagekräftigen Identifier (vgl. Abschnitt 5.3) Hashcodes erzeugt werden, die als Identifier für die Kommunikation über das Internet verwendet werden.

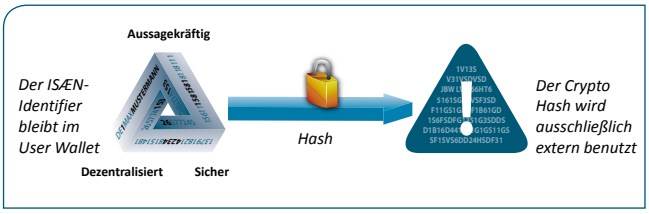

Abbildung 7: ISÆN und Zookos Dreieck

Die Bestandteile des ISÆN-Identifiers (vgl. Abschnitt 3.4) sind die persönlichen Daten des Nutzers (angedacht ist auch die Verwendung von biometrischen Merkmalen) und sollen immer in dessen Hand bzw. in einem abgesicherten Bereich der Ævatar-App bleiben. Sie werden ausschließlich verwendet, um daraus mit einem geeigneten kryptographischen Verfahren einen Hashwert zu generieren. Bei der Kommunikation mit Diensten soll ausschließlich dieser Hashwert als Identifier verwendet werden. Hier muss durch geeignete

Anwendung des Hashverfahrens und weiterer kryptographischer Verfahren gewährleistet werden, dass der bei der Kommunikation mit Diensten verwendete Identifier die gewünschten Sicherheits- und Dezentralitätseigenschaften hat.

3.4 Aufbau des ISÆN-Identifiers

Die Standardisierungsinitiative ISÆN soll die rechtssichere Weitergabe und Verarbeitung von persönlichen Daten sowohl in kommerziellen als auch im behördlichen Umfeld erleichtern und absichern. ISÆN adressiert in erster Linie den automatischen Datenaustausch und die Verarbeitung der Daten, die Kennung kann aber natürlich auch in gedruckter Form (beispielsweise als QR-Code) verwendet werden, um beispielsweise Dokumente auszutauschen.

Es wurde vorgeschlagen den ISÆN-Identifier wie folgt aufzubauen:

- Code des Geburtslandes
- Geschlecht
- Nachname
- Vorname
- Geburtsdatum
- Postleitzahl des Geburtsortes
- Mobilfunknummer
- Gültigkeitsdauer (beispielsweise geänderte ISÆN bei Wechsel der Mobilfunknummer)
- biometrischer Hash oder Fingerabdruck, „Selfie“ zur Absicherung der Daten

Beispiel für einen solchen ISÆN-Identifier:

DE2MUSTERMANNERIKA196904010157812345678

DE	Deutschland
2	Weiblich
Mustermann	Nachname
Erika	Vorname
01.04.1969	Geburtsdatum
0157812345678	Mobilfunknummer

Durch die Erweiterung des ISÆN-Identifiers mit einer textuellen Repräsentation biometrischer Merkmale sollen Dritte, denen die anderen Daten über eine betroffene Person zu Verfügung stehen, nicht den kompletten ISÆN-Identifier und damit nicht den ISÆN-Hash konstruieren können.

4 Rechtliche Grundlagen

An dieser Stelle soll das Vorhaben in den rechtlichen Kontext eingebettet werden. Hierzu werden nachfolgend die eIDAS-Verordnung und die neue EU-Datenschutz-Grundverordnung vorgestellt, da das nationale Recht hierdurch verdrängt wird. Im Hinblick darauf wird auf eine detaillierte Beschreibung nationaler Vorschriften verzichtet.

4.1 eIDAS-Verordnung

Am 01.07.2016 ist die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS-Verordnung (EU) Nr. 910/2014)[3] in Kraft getreten. Die Verordnung schafft für den öffentlichen Bereich europäische Regelungen für elektronische Signaturen, Siegel und Zeitstempel und soll insoweit einen einheitlichen Umgang mit diesen Vertrauensdiensten im neu etablierten digitalen Binnenmarkt ermöglichen. Als Verordnung gilt sie unmittelbar in den Mitgliedsstaaten und bedarf daher keiner weiteren Umsetzung. Sie ersetzt die EU-Signaturrichtlinie. Das Signaturgesetz und die Signaturverordnung bleiben weiterhin anwendbar, sofern sie keine widersprechenden Regeln treffen.

Die eIDAS-Verordnung schafft einen einheitlichen europäischen Binnenmarkt für Sicherungsmittel, mit dem Ziel, die Sicherheit, Vertraulichkeit und Integrität von Daten sowie die Identität der Kommunikationspartner zu ermöglichen. Gerade im elektronischen Rechtsverkehr müssen Anwender den bereitgestellten Diensten vertrauen können. Aus diesem Grund sind technische Lösungen entwickelt worden, die auf der Grundlage einer zertifikatbasierten Infrastruktur eine sichere Basis schaffen. Die Angebote reichen mittlerweile von elektronischen Signaturen über die Authentifizierung von Websites bis hin zu elektronischen Postversanddiensten.[4]

Die Verordnung regelt zum einen die Koordination nationaler Systeme zur elektronischen Identifizierung (Art. 6 bis 12) und die unionseinheitliche Regelung von Vertrauensdiensten (Art. 13 bis 45). Zum anderen bestehen in verschiedenen Anhängen (I, II, III und IV) Anforderungslisten für qualifizierte Zertifikate für elektronische Signaturen, qualifizierte Signaturerstellungseinheiten, elektronische Siegel und Website-Authentifizierung.

4.1.1 Anwendungsbereich

Der Anwendungsbereich der eIDAS-Verordnung erstreckt sich gemäß Art. 2 Abs. 1 (EU) Nr. 910/2014 auf Vertrauensdienstanbieter, die in der Union niedergelassen sind, und notifizierte elektronische Identifizierungssysteme. Vertrauensdienste innerhalb geschlossener Systeme wie beispielsweise interne Verfahren, die aufgrund freiwilliger privatrechtlicher Vereinbarung ergehen, sind nach Art. 2 Abs. 2 (EU) Nr. 910/2014 von der Verordnung ausgenommen. Die Verordnung findet ebenfalls keine Anwendung auf Sachverhalte im Zusammenhang mit dem Abschluss und der Gültigkeit von Verträgen oder anderen rechtlichen Verpflichtungen, für die nach nationalem oder Unionsrecht Formvorschriften zu erfüllen sind, siehe Art. 2 Abs. 3 (EU) Nr. 910/2014.

4.1.2 Elektronische Identifizierung

Neben den Anforderungen an Vertrauensdienste in Kapitel III befasst sich die Verordnung in Kapitel II mit der elektronischen Identifizierung. Diese wird in Art. 3 Nr. 1 (EU) Nr. 910/2014 als ein „Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine natürliche Person, die eine juristische Person vertritt, eindeutig repräsentieren“ juristisch definiert. Der Kernregelungsgehalt ist die grenzübergreifende Einsetzbarkeit. Konkrete Ausgestaltungsanforderungen sowohl für die Mittel selbst als auch für die Ausgabestellen werden nicht gestellt.[5]

Die eIDAS-Verordnung enthält in Art. 6 (EU) Nr. 910/2014 eine Anerkennungspflicht in Bezug auf alle ausländischen staatlichen Identifizierungswerkzeuge

eines Mitgliedsstaats, die für diejenigen Dienste innerhalb eines anderen Mitgliedsstaats notifiziert wurden, die eine elektronische Identifizierung vorsehen. Art. 6 (EU) Nr. 910/2014 verlangt damit von jedem Mitgliedsstaat, der für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst ein elektronisches Identifizierungssystem fordert, auch alle anderen Identifizierungssysteme aus anderen Mitgliedsstaaten anzuerkennen, die bei der Kommission notifiziert und nach Art. 9 Abs. 2 (EU) Nr. 910/2014 im Amtsblatt der Europäischen Union veröffentlicht wurden. Des Weiteren muss das Sicherheitsniveau des betreffenden elektronischen Identifizierungsmittels gemäß Art. 6 Abs. 1 lit. b (EU) Nr. 910/2014 so hoch wie oder höher als das von der einschlägigen öffentlichen Stelle für den Zugang zu diesem Online-Dienst geforderte Sicherheitsniveau sein, wenn dieses dem Sicherheitsniveau „Substanziell" oder „Hoch" entspricht. Die Sicherheitsniveaus werden in Art. 8 Abs. 2 (EU) Nr. 910/2014 näher definiert.

Die gegenseitige Anerkennung mitgliedsstaatlicher Identifizierungssysteme stellt eine erhebliche Erweiterung der Signaturrichtlinie dar. In Art. 7 (EU) Nr. 910/2014 werden die Voraussetzungen für die Notifizierung geregelt.[6] Danach ist ein Identifizierungssystem notifizierbar, wenn der in Art. 7 (EU) Nr. 910/2014 genannte Katalog mit acht Anforderungen kumulativ erfüllt ist. Beispielhaft sollen die wichtigsten Anforderungen vorgestellt werden. Gemäß Art. 6 Abs. 1 lit. a (EU) Nr. 910/2014 müssen die elektronischen Identifizierungsmittel vom notifizierenden Mitgliedsstaat ausgestellt werden (I), im Auftrag des notifizierenden Mitgliedsstaats ausgestellt (II) oder unabhängig vom notifizierenden Mitgliedsstaat ausgestellt und von diesem anerkannt werden (III). Ferner müssen sie von mindestens einem Dienst verwendet werden, der von einer öffentlichen Stelle bereitgestellt wird und für den eine elektronische Identifizierung erforderlich ist (Art. 7 lit. b (EU) Nr. 910/2014). Zusammenfassend zeigt sich, dass sich die Identifizierungssysteme auf den E-Government-Bereich beziehen. In Erwägungsgrund 17 wird dies umso mehr deutlich, als hier der Privatsektor direkt adressiert wird. Danach heißt es, dass die Mitgliedsstaaten den Privatsektor dazu ermutigen sollten, freiwillig elektronische Identifizierungsmittel im Rahmen eines notifizierten Systems zu Identifizierungszwecken zu verwenden, wenn dies für Online-Dienste oder Transaktionen nötig ist.

In Kapitel II der eIDAS-Verordnung werden die Folgen von Sicherheitsverletzungen sowie Regelungen zur Haftung festgelegt.

4.1.2.1 Vertrauensdienste

Die Verordnung unterscheidet zwischen Vertrauensdiensten und qualifizierten Vertrauensdiensten.

Vertrauensdienste sind nach Art. 3 Abs. 16 (EU) Nr. 910/2014 elektronische Dienste, die in der Regel gegen Entgelt erbracht werden und aus der Erstellung, Überprüfung und Validierung von elektronischen Signaturen, Zeitstempeln, Siegeln und Zertifikaten bestehen. Darüber hinaus gelten Dienste, die sich mit der Erstellung, Überprüfung und Validierung für die Website-Authentifizierung, der Zustellung elektronischer Einschreiben oder der Bewahrung von elektronischen Signaturen, Siegeln oder Zertifikaten befassen, ebenfalls als Vertrauensdienste. Ziel der Verordnung ist gemäß Erwägungsgrund 24 das freie Zirkulieren derartiger Vertrauensdienste im Binnenmarkt, wenn sie den Anforderungen der Verordnung entsprechen.

Ein qualifizierter Vertrauensdienst ist entsprechend Art. 3 Abs. 17 (EU) Nr. 910/2014 ein Vertrauensdienst, der die einschlägigen Anforderungen der Verordnung erfüllt. Qualifizierte und nichtqualifizierte Vertrauensdienstanbieter müssen gemäß Art. 19 Abs. 1 (EU) Nr. 910/2014 geeignete technische und organisatorische Maßnahmen zur Beherrschung der im Zusammenhang mit den erbrachten Vertrauensdiensten entstehenden Sicherheitsrisiken ergreifen. Die Maßnahmen müssen

dabei den jeweils neusten Stand der Technik gewährleisten.

4.1.3 Elektronische Signaturen

Im Rahmen der Signaturen wird zusätzlich zwischen den fortgeschrittenen und aus dem deutschen Signaturrecht bereits bekannten qualifizierten elektronischen Signaturen differenziert. Neben den Vorschriften Art. 13–24 regeln die Art. 25–34 und der Anhang I, II entsprechende Anforderungen für elektronische Signaturen und Signaturerstellungseinheiten.

Gemäß Art. 25 Abs. 1 (EU) Nr. 910/2014 darf einer elektronischen Signatur die Rechtswirkung und Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt. Hinsichtlich qualifizierter elektronischer Signaturen stellt Art. 25 Abs. 2 (EU) Nr. 910/2014 klar, dass diese die gleiche Rechtswirkung wie eine handschriftliche Unterschrift haben. Eine Beweisregelung gibt es für qualifizierte elektronische Signaturen hingegen nicht. Nach EWG 49 bleibt es den Mitgliedsstaaten vorbehalten, die Rechtswirkung von elektronischen Signaturen festzulegen. Damit gilt für diese die Regelung des § 371 a ZPO.[7]

4.1.4 Elektronische Siegel

Während elektronische Signaturen für natürliche Personen gelten, wird auch juristischen Personen das Signieren in Form so genannter elektronischer Siegel ermöglicht. Das elektronische Siegel ist damit eine elektronische Signatur einer juristischen Person. Die Anforderungen an elektronische Siegel finden sich im Anhang III sowie in den Art. 35–40, wobei explizit auf die Vorschriften Art. 29–34 verwiesen wird.

Im Gegensatz zu den elektronischen Signaturen wird für qualifizierte Siegel gemäß Art. 35 Abs. 2 (EU) Nr. 910/2014 die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe zugesprochen.

4.1.5 Elektronische Zeitstempel

Nach Art. 3 Nr. 33 (EU) Nr. 910/2014 sind elektronische Zeitstempel Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren. Qualifizierte elektronische Zeitstempel wiederum sind solche, die die Anforderungen des Art. 42 erfüllen, Art. 3 Nr. 34 (EU) Nr. 910/2014. Qualifizierte Zeitstempel waren im SigG enthalten, nicht jedoch in der SigRL.

Auch für qualifizierte Zeitstempel gilt gemäß Art. 41 Abs. 2 (EU) Nr. 910/2014 die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben ist, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

4.1.6 Elektronische Einschreiben

Regelungen zum elektronischen Einschreiben finden sich in Art. 43 (EU) Nr. 910/2014 und Art. 44 (EU) Nr. 910/2014. Die Legaldefinition erfolgt in Art. 3 Abs. 36 (EU) Nr. 910/2014.

4.1.7 Website-Authentifizierung

Für die Website-Authentifizierung gelten die Vorschrift des Art. 45 (EU) Nr. 910/2014 und der Anhang IV. Qualifizierte Zertifikate müssen von einem qualifizierten Vertrauensdienstanbieter ausgestellt werden, wobei hierfür vertrauenswürdige Mindestanlagen und deren Sicherung durch eine fortgeschrittene Signatur oder ein fortgeschrittenes Siegel notwendig sind.[8]

4.2 Datenschutz-Grundverordnung

Das Datenschutzrecht wird künftig einheitlich europaweit durch die Datenschutz-Grundverordnung (DSGVO) geregelt. Am 24.05.2016 ist die Datenschutz-Grundverordnung (EU) 2016/679 in Kraft getreten. Gemäß

Art. 99 Abs. 2 (EU) 2016/679 erlangt sie ihre unmittelbare Geltung jedoch erst zwei Jahre nach ihrem Inkrafttreten, und damit ab dem 25.05.2018. Mit dem Tag des Inkrafttretens wird sie die derzeit noch geltende EU-Datenschutzrichtlinie ablösen, weite Teile des Bundesdatenschutzgesetzes ersetzen und insgesamt einen einheitlichen, unionsweiten datenschutzrechtlichen Rahmen schaffen.

Anders als die EU-Richtlinie bedarf die Datenschutz-Grundverordnung (DSGVO) keines weiteren Umsetzungsakts. Sie genießt gegenüber den dann noch bestehenden nationalen Datenschutzvorschriften Anwendungsvorrang, Art. 288 AEUV. Gleichwohl enthält die Verordnung mehr als 60 Öffnungsklauseln, die den Mitgliedsstaaten insoweit einen eigenen Regelungsspielraum lassen werden.[9]

Die DSGVO regelt die Verarbeitung personenbezogener Daten zum Schutz natürlicher Personen sowie ausweislich des Art. 1 Abs. 1 (EU) 2016/679 auch den freien Verkehr solcher Daten. Im Gegensatz zum BDSG betrachtet die DSGVO daher neben persönlichkeitsrechtlichen auch wirtschaftliche Aspekte und schützt diese im Rahmen von Abwägungsentscheidungen. Nachfolgend sollen die wesentlichen Neuerungen kurz skizziert werden.

Eine der gewichtigsten Änderungen ist die Einführung des Marktortprinzips. Zwar hatte der EuGH in der „Google-Spain-Entscheidung“[10] das Marktortprinzip bereits teilweise vorweggenommen, die Regelung findet sich jedoch nunmehr explizit in Art. 3 II (EU) 2016/679. Danach wird der Anwendungsbereich der Verordnung auch auf Verantwortliche ausgedehnt, die keine Niederlassung in der EU haben, sofern sie Personen in der Union Waren oder Dienstleistungen anbieten (lit. a) oder das Verhalten betroffener Personen beobachten (lit. b). Letzteres liegt insbesondere beim Profiling vor. Die DSGVO bezweckt auch eine Stärkung der Betroffenenrechte wie das so genannte Recht auf Vergessenwerden, das Recht auf Datenportabilität und das Auskunftsrecht. Daneben werden auch die Informationspflichten erheblich erhöht. So ist der Katalog der Informationen, die der betroffenen Person zur Verfügung zu stellen sind, erweitert worden. Das Recht auf Vergessenwerden ist letztlich als schlichtes Löschrecht ausgestaltet worden.[11] Nach Art. 17 Abs. 1 DSGVO hat die betroffene Person die Möglichkeit, aus bestimmten Gründen die Löschung der personenbezogenen Daten zu veranlassen. Dies kann beispielsweise der Fall sein, wenn der Zweck für die Datenerhebung oder -verarbeitung entfallen ist (vgl. Art. 17 Abs. 1a DSGVO). Die Verpflichtung zur Löschung wird flankiert durch Hinweis- und Informationspflichten des Verantwortlichen, der im Fall, dass er die Daten öffentlich gemacht hat, unter bestimmten Bedingungen weitere Verantwortliche darüber in Kenntnis setzen muss, dass die betroffene Person die Löschung aller Links zu den personenbezogenen Daten verlangt hat (vgl. Art. 17 Abs. 2 DSGVO). Des Weiteren eröffnet das Recht auf Datenportabilität betroffenen Personen die Möglichkeit, die von ihnen zur Verfügung gestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Die Vorschrift zielt in erster Linie auf eine Vereinfachung, um Profile in sozialen Netzwerken oder E-Mail-Konten bei einem Wechsel zu einem anderen Anbieter transferieren zu können.[12] Das Auskunftsrecht enthält auch deutliche Erweiterungen zum nationalen Recht, da es u. a. ebenfalls regelt, dass der Verantwortliche im Rahmen der Auskunftserteilung immer eine Kopie der personenbezogenen Daten der betroffenen Person, die Gegenstand der Verarbeitung ist, bereitstellen muss. Die Bereitstellung muss unentgeltlich und in einem gängigen elektronischen Format unter Beachtung der Rechte Dritter erfolgen, siehe Art. 15 Abs. 3 (EU) 2016/679. Des Weiteren erstreckt sich die Auskunftspflicht auch auf die geplante Speicherdauer von Daten, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerruf, das Bestehen eines Beschwerderechts bei einer

Aufsichtsbehörde sowie die Bezeichnung der geeigneten Garantien gemäß Art. 46 zur Wahrung eines angemessenen Datenschutzniveaus bei Übermittlungen in Drittländer.

Im Übrigen sieht die DSGVO für Verantwortliche und Auftragsverarbeiter deutlich erweiterte Nachweispflichten vor, wonach gemäß Art. 5 Abs. (EU) 2016/679 der für die Verarbeitung Verantwortliche belegen muss, dass er die in Art. 5 Abs. 1 (EU) 2016/679 verankerten Datenschutzgrundsätze eingehalten hat.

Die Datenschutz-Grundverordnung fördert den Einsatz von datenschutzumsetzenden Techniklösungen im Rahmen der Entwicklungsphase. Mit dem in Art. 25 Abs. 1, 2 (EU) 2016/679 geregelten „Privacy by Design“ und „Privacy by Default“ sollen IT-Systeme so ausgestaltet werden, dass sie die Datenschutzgrundsätze wirksam umsetzen. Darüber hinaus sollen sie so voreingestellt sein, dass sie nur solche Daten verarbeiten, deren Verarbeitung für den verfolgten Zweck erforderlich ist. Ferner führt die DSGVO die Datenschutz-Folgeabschätzung ein, die die bisherige Vorabkontrolle ablöst.

Weitere Regelungen betreffen das Kopplungsverbot im Rahmen von Einwilligungen und mögliche Zweckänderungen bei Vereinbarkeit mit dem Ursprungszweck.

Die DSGVO enthält auch erhebliche prozedurale Änderungen gegenüber der Datenschutz-RL von 1995. Zu nennen sind hier insbesondere die erheblich stärker ausdifferenzierten Bestimmungen zu den unabhängigen Datenschutzaufsichtsbehörden und zu deren Zusammenwirken in einer EU-Datenschutzgruppe, die bei divergierenden Positionen der Aufsichtsbehörden mehrheitlich entscheiden kann. Zudem werden ihre Sanktionsbefugnisse gestärkt und vereinheitlicht. Geldbußen können zukünftig bis zu 20 Millionen Euro bzw. vier Prozent des weltweiten Jahresumsatzes des rechtsverletzenden Unternehmens betragen (vgl. Art. 83 Abs. 5 DSGVO), während der Bußgeldrahmen des deutschen Datenschutzrechts bislang auf 300.000 Euro begrenzt ist. Auch die Haftung sowohl von Verantwortlichen als auch von Auftragsverarbeitern für immaterielle Schäden stellt eine ausdrückliche Erweiterung dar.[13]

Das im deutschen Recht bereits bekannte Prinzip der Bestellung eines betrieblichen Datenschutzbeauftragten wird europaweit festgelegt (vgl. Art. 37 f. DSGVO), wobei allerdings die Ausgestaltung der Bestellungspflicht durch nationales Recht weiterhin möglich bleibt.

Bis zur Anwendung der DSGVO am 25. Mai 2018 sind in Deutschland noch zahlreiche Anpassungen vorzunehmen, die sowohl das Datenschutzrecht des Bundes als auch die Datenschutzbestimmungen der Länder betreffen. Allein auf Bundesebene sind ca. 300 Gesetze zu überprüfen, die Datenschutzregelungen enthalten.[14]

4.3 Nationales Recht

Im Hinblick auf die DSGVO, die ab dem 25.05.2018 unmittelbar in allen EU-Mitgliedsstaaten gilt, wird auf eine detaillierte Beschreibung der derzeitigen deutschen Rechtslage im Bereich des Datenschutzes verzichtet.

Das deutsche Datenschutzrecht basiert auf der Rechtsprechung des Bundesverfassungsgerichts zur informationellen Selbstbestimmung[15] und unterscheidet zwischen allgemeinen und bereichsspezifischen Datenschutzregelungen. Die allgemeinen Datenschutzregelungen (Bundesdatenschutzgesetz und Datenschutzgesetze der Länder) werden durch die DSGVO weitgehend abgelöst. Unklar ist derzeit das Schicksal der bereichsspezifischen Datenschutzregelungen, die aufgrund des subsidiären Charakters des BDSG und der Landesdatenschutzgesetze diesen grundsätzlich

vorgehen. Da die DSGVO den nationalen Gesetzgebern in bestimmten Bereichen Regelungsspielräume lässt (etwa beim Datenschutz im Beschäftigungsverhältnis, bei Gesundheitsdaten und bei Statistik, Wissenschaft und Forschung), ist zu erwarten, dass es auch weiterhin ein bereichsspezifisches deutsches Datenschutzrecht geben wird. Zudem ist zu erwarten, dass die EU-Regelungen für den Datenschutz in der Telekommunikation und im Internet, die bisher in der Datenschutzrichtlinie für elektronische Kommunikationsdienste (ePrivacy-RL),[16] die dem Telekommunikationsgesetz und dem Telemediengesetz zugrunde liegt, überarbeitet und gegebenenfalls durch eine EU-Verordnung ersetzt werden.

5 Überblick über Identifikationssysteme in Deutschland

Identifikationssysteme dienen dazu, eine Person oder ein Objekt eindeutig zu identifizieren. Im nachfolgenden Abschnitt werden verschiedene Identifikationssysteme zur Identifikation von Personen und deren Merkmale vorgestellt.

5.1 Elektronischer Personalausweis

Der neue Personalausweis hat am 01.11.2010 den alten Personalausweis abgelöst. Im Gegensatz zu diesem stellt der neue Personalausweis mit Hilfe eines RFID-Chips eine Vielzahl von elektronischen Funktionalitäten bereit. Dazu gehören die biometriegestützte Identifikation gegenüber Behörden, elektronische Authentifizierung gegenüber Dritten („eID-Funktion“) und die Möglichkeit der Ausstellung einer (kostenpflichtigen) qualifizierten elektronischen Signatur entsprechend dem Signaturgesetz.

Die folgenden Informationen werden digital auf dem Ausweis gespeichert:

- Familienname
  - Gegebenenfalls Doktortitel
  - Gegebenenfalls Ordens- bzw. Künstlername
- Vorname(n)
- Geburtsdatum
- Geburtsort
- Anschrift mit Postleitzahl
- Lichtbild
- Seriennummer
- optional zwei Fingerabdrücke

Körpergröße, Augenfarbe und Unterschrift werden nicht digital gespeichert.

Mit Hilfe der so genannten AusweisApp können sich Benutzer im Internet gegenüber Dritten eindeutig identifizieren. Dafür wird ein elektronisches Lesegerät benötigt und zur Verhinderung von Missbrauch muss vor der Nutzung eine PIN eingegeben werden. Dienstanbieter, die die Authentifizierung über die eID-Funktion bereitstellen wollen, haben die Wahl, selbst einen eID-Server zu betreiben oder einen externen Server zu mieten und diesen in die eigene Anwendung zu integrieren. Dienstanbieter, die eID-Funktionen bereitstellen, müssen dazu bei einer zentralen Bundesstelle (unter Angabe der Information, auf welche Datenfelder des Personalausweises zugegriffen werden soll, und des jeweiligen Grundes dafür) ein elektronisches Zertifikat beantragen. Mit diesem Zertifikat, in dem auch gespeichert ist, für welche Daten eine Zugriffsberechtigung erteilt wurde, authentifizieren sie sich zunächst gegenüber dem Personalausweis. Die privaten Schlüssel dafür müssen in einem zertifizierten Hardware-Sicherheitsmodul gespeichert werden und dürfen dieses Modul nicht verlassen. Anschließend authentifiziert sich auch der Personalausweis mittels eines Zertifikats gegenüber dem Dienstanbieter. Über die Eingabe seiner PIN kann der Benutzer dann die Übertragung der angeforderten Daten starten.

Ähnlich der geplanten Funktionalität des ISÆN-Identifiers bietet die eID-Funktionalität des elektronischen Personalausweises die Möglichkeit der eindeutigen und universellen Identifizierung eines Nutzers. Dieses Merkmal unterscheidet den elektronischen Personalausweis von anderen Identifikationssystemen, die nur bereichsspezifisch sind und deren Verwendung außerhalb des jeweiligen Bereichs unzulässig ist. Im Gegensatz zu ISÆN wird die Identifizierung durch den Personalausweis nicht durch persönliche Daten, sondern durch kryptographische Maßnahmen erreicht.

5.2 Sozialversicherungsnummer

Die Sozialversicherungsnummer dient der persönlichen Identifikation von Versicherten im Sozialversicherungswesen und besteht aus einer zwölfstelligen Zeichenkette. In Deutschland muss hierbei aus Gründen des Datenschutzes zwischen der Krankenversichertennummer (siehe Abschnitt „Gesundheitskarte“) und der Rentenversicherungsnummer, mit der Versicherte der gesetzlichen Rentenversicherung identifiziert werden, unterschieden werden.

Die Sozialversicherungsnummer ist gemäß § 147 SGB VI wie folgt aufgebaut:

- Bereichsnummer des Rentenversicherungsträgers, 1–2 Stellen
- Geburtstag des Versicherten, 2 Stellen
- Geburtsmonat des Versicherten, 2 Stellen
- Geburtsjahr des Versicherten, 2 Stellen
- Anfangsbuchstabe des Geburtsnamens des Versicherten, 1 Stelle
- Seriennummer (00–49 = männlich, 50–99 = weiblich oder unbestimmtes Geschlecht), 2 Stellen
- Prüfziffer, 1 Stelle

Die Sozialversicherungsnummer darf nur für den vorgesehenen Einsatzzweck verwendet werden und ist somit kein geeignetes universelles Identifizierungsmerkmal.

5.3 Steueridentifikationsnummer

Die steuerliche Identifikationsnummer (IdNr) ist eine bundeseinheitliche und dauerhafte Identifikationsnummer von in Deutschland gemeldeten Bürgern für Steuerzwecke. Sie besteht aus zehn zufällig gebildeten Ziffern (welche keinen Rückschluss auf den Steuerpflichtigen selbst zulassen) und einer Prüfziffer. Sie wird über die Kommunalverwaltungen verteilt, kann jedoch bei Verlust beim zuständigen Finanzamt erneut erfragt werden. Andere Stellen als die Finanzbehörden dürfen diese Nummer nur erheben und verwenden, soweit es für eine Datenübertragung zwischen ihnen und den Finanzbehörden erforderlich ist.

Die IdNr ermöglicht beispielsweise elektronisch bereitgestellte (vorausgefüllte) Steuererklärungsformulare zu verwenden sowie die automatisierte Verarbeitung elektronischer Belege. Im Gegensatz zur Steuernummer, die sich beispielsweise bereits ändert sobald ein Bürger innerhalb der Stadt bezirksübergreifend umzieht, bleibt die IdNr eines Bürgers ein Leben lang gleich (die Daten werden spätestens 20 Jahre nach dem Tod des Steuerpflichtigen gelöscht). Eine IdNr erhalten sowohl Personen mit einem Wohnsitz in Deutschland als auch Personen, die zwar nicht melderechtlich erfasst, jedoch in Deutschland steuerpflichtig sind. Auch Kinder (der Sache nach natürliche Personen, die in Deutschland ihren Wohnsitz oder gewöhnlichen Aufenthalt haben) erhalten eine IdNr.

Genau wie bei der Sozialversicherungsnummer ist die Verwendung der IdNr streng an einen Zweck (Steuerangelegenheiten) gebunden, diese darf daher nicht als universelles Identifikationsmerkmal verwendet werden.

5.4 Gesundheitskarte

In Deutschland gilt seit Januar 2015 für die Inanspruchnahme von Leistungen aus der gesetzlichen Krankenkasse die elektronische Gesundheitskarte (eGK), die auch innerhalb der EU ihre Gültigkeit behält. Neben den auf der Gesundheitskarte gespeicherten medizinischen Daten (siehe weiter unten) werden auch personenbezogene Daten des Versicherungsnehmers gespeichert. Die eGK enthält u. a. ein Lichtbild des Versicherungsnehmers und dessen Geschlecht. Haben sich die Anschrift oder sonstige Kontaktdaten des Versicherungsnehmers geändert und wurde die entsprechende Krankenkasse darüber informiert, so ist es möglich, diese Angaben beim nächsten Arztbesuch beim Auslesen der Gesundheitskarte zu aktualisieren. Die Ausstellung (und Zusendung) einer neuen Gesundheitskarte für einen Versicherungsnehmer mit veränderter Anschrift ist damit nicht mehr nötig.

Auf Wunsch des Versicherten können auf der Gesundheitskarte auch Notfalldaten gespeichert werden. Diese können sich beispielsweise auf Allergien oder auf für eine etwaige Behandlung relevante Vorerkrankungen beziehen.

Auf der eGK sind gemäß § 291 Abs. 2 SGB V mindestens die folgenden Informationen enthalten:

- die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die Kassen-

ärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat
- Familienname und Vorname(n) des Versicherten
- Geburtsdatum
- Geschlecht
- Anschrift
- Krankenversichertennummer
- Versichertenstatus, für Versichertengruppen nach § 267 Abs. 2 Satz 4 SGB V in einer verschlüsselten Form
- Zuzahlungsstatus
- Tag des Beginns des Versicherungsschutzes
- bei befristeter Gültigkeit der Karte das Datum des Fristablaufs

Die Krankenversichertennummer besteht aus einem unveränderlichen Teil und einem veränderlichen Teil, der die Kassenzugehörigkeit und gegebenenfalls Daten zum Hauptversicherten enthält.

Die eGK enthält digitale Zertifikate, die für jeden Versicherten individuell erzeugt werden. Die aktuelle Länge der kryptographischen Schlüssel beträgt 2048 Bit. Zum Entschlüsseln der auf der Karte verschlüsselt gespeicherten Informationen muss sich der Versicherte gegenüber der Karte mit einer PIN authentifizieren.

6 Technische Grundlagen

6.1 Hashfunktionen

Hashfunktionen bilden Zeichenketten beliebiger Länge auf Zeichenketten einer festen Länge ab, auch „Hashwert“ oder „Hash“ genannt. Eine spezielle Klasse von Hashfunktionen sind kryptographische Hashfunktionen, welche die folgenden zusätzlichen Eigenschaften besitzen:

- Einwegfunktion: Das Urbild eines Hashwertes kann nur mit nicht vertretbar großem Aufwand berechnet werden.
- Kollisionsresistenz: Zwei Urbilder mit gleichem Hashwert können nur mit nicht vertretbar großem Aufwand gefunden werden.

Kryptographische Hashfunktionen finden Anwendung beispielsweise bei der Integritätsprüfung von Daten, bei digitalen Signaturen und bei Blockchiffren.

Bei ISÆN sollen kryptographische Hashfunktionen eingesetzt werden, um aus einer Zeichenkette mit personenbezogenen Daten einen eindeutigen Identifier zu erzeugen.

6.2 Blockchain

Mit zunehmender Bekanntheit der digitalen Währung „Bitcoin“ wurde auch die zugrunde liegende Blockchain-Technologie einer breiteren Öffentlichkeit bekannt. Im Folgenden werden nach einer kurzen Einführung die Nutzung der Blockchain im Kontext von Bitcoin sowie weitere Anwendungen beschrieben.

6.2.1 Blockchain-Technologie

Eine Blockchain ist ein Speicher, in dem Daten redundant bei allen teilnehmenden Parteien gespeichert werden. Jede Partei besitzt somit eine Kopie der gesamten Blockchain. Zusammen bilden die teilnehmenden Parteien das Blockchain-Netzwerk. Daten werden in einzelnen Blöcken gespeichert. Zusätzlich enthält jeder Block einen Hashwert des vorherigen Blocks und einen Zeitstempel. Hierdurch entsteht ein Baum von Blöcken.[17] Weitere Eigenschaften der Blockchain sind:

- Nur die längste Kette von Blöcken ist gültig.
- Das Anfügen eines neuen Blocks ist rechenintensiv.[18]
- An die Blockchain werden stetig neue Blöcke angefügt.

Kann keine Partei über einen Zeitraum hinweg schneller neue Blöcke anfügen als der Rest des Netzwerks, wird die Blockchain zu einem Permanentspeicher, d. h., einmal gültige Blocke können nachträglich nicht mehr geändert werden. Hierdurch eignet sich die Blockchain für die Dokumentation von Transaktionen, insbesondere wenn auf eine zentrale Vertrauensinstanz verzichtet werden soll.

Durch den Erfolg der digitalen Währung „Bitcoin“ (vgl. Abschnitt 6.2.2) wurde die Blockchain als Speicher für Transaktionen bekannt und wird heute in vielen Anwendungsszenarien (Finanztransaktionen, Energiehandel, Datenhandel) als technische Lösung diskutiert. Start-ups wie auch etablierte Unternehmen arbeiten gemeinsam an Anwendungen mit der Blockchain.

6.2.2 Nutzung der Blockchain bei Bitcoin

Bei Bitcoin dient die Blockchain zur Realisierung eines dezentralen Kassenbuchs (auch „Distributed Ledger“ genannt), in dem alle Transaktionen aufgezeichnet werden. Im Gegensatz zum herkömmlichen Geldtransfer haben die Nutzer keine eigenen Konten, sondern treten lediglich als Sender oder Empfänger von Transaktionen auf.

Bei Bitcoin entstehen neue Blöcke durch den Vorgang des so genannten Minings, etwa alle 10 Minuten wird ein neuer Block an die Blockchain angefügt. Die Gesamtrechenleistung des Bitcoin-Netzwerks hängt direkt von dessen Teilnehmern ab. Aktuell nimmt sie durch neue Teilnehmer und bessere Hardware ständig zu. Daher überprüft das Netzwerk alle zwei Wochen, wie viel Zeit im Mittel zwischen dem Erzeugen zweier gültiger Blöcke vergangen ist, und passt daraufhin die Komplexität der zu lösenden kryptographischen Auf-

gabe so an, dass diese Zeit konstant bleibt. Da es möglich ist, dass von verschiedenen Minern neue Blöcke parallel erzeugt werden, wird ein Konsens darüber benötigt, welcher dieser „konkurrierenden" Blöcke der gültige ist. Dieser Konsens wird durch die Bestätigung eines Blockes erreicht. Ein Block wird bestätigt, indem ein neuer Block an ihn bzw. an seine Kette angefügt wird. Alle Transaktionen, die in einem Block gespeichert sind, der nicht der längsten Kette angehört, müssen der längsten Kette als neue Transaktionen angefügt werden, damit sie gültig sind.

Als Anreiz, am Bitcoin-Netzwerk teilzunehmen und nur die längste Kette zu erweitern, erhalten Miner, die gültige Blöcke erzeugt haben, eine Belohnung in Form von Bitcoins. Zusätzlich zur Belohnung für das Anfügen eines gültigen Blocks erhält der Miner die Gebühren der darin enthaltenen Transaktionen. Der Sender einer Transaktion kann diese Gebühr festlegen und dadurch einen Anreiz schaffen, seine Transaktion schneller in einem neuen Block an die Blockchain anzufügen. Bevor transferierte Bitcoins verwendet werden können, benötigt die entsprechende Transaktion eine bestimmte Anzahl von Bestätigungen. Eine Transaktion wird bestätigt, indem der Block, der sie enthält, bestätigt wird. Damit soll sichergestellt werden, dass der Block mit der Transaktion gültig bleibt. Bis überwiesene Bitcoins vom Empfänger genutzt werden können, vergehen derzeit etwa 60 Minuten.

Das Bitcoin-Netzwerk ist öffentlich zugänglich, jede Transaktion ist nachvollziehbar. Bei Bitcoin verwenden Nutzer deshalb Pseudonyme. In dieses Pseudonym, auch „Bitcoin-Adresse" genannt, geht der öffentliche Teil eines kryptographischen Schlüsselpaars (der „Public Key") ein. Mittels des zugehörigen privaten Schlüssels (des „Private Keys") kann der Inhaber beweisen, dass ihm eine bestimmte Adresse gehört. Eine Bitcoin-Adresse soll keine Rückschlüsse auf die Identität des Nutzers zulassen. Tatsächlich ist dieses Pseudonym jedoch nur bedingt anonym.[19]

6.2.3 Weitere Anwendungen der Blockchain

Grundsätzlich eignen sich Blockchains jedoch zum Verwalten der Übertragung unterschiedlichster Daten. So wurde im Rahmen von Ethereum eine Blockchain entwickelt, die die Ausführung digitaler Verträge ermöglicht (siehe Abschnitt 6.2.4). Unter dem Begriff „Blockchain" werden heute verschiedene Implementierungen für unterschiedliche Einsatzszenarien zusammengefasst. Gemeinsam ist den Varianten, dass sie zur Protokollierung von Transaktionen eingesetzt werden und auf einer P2P-Netzwerktopologie basieren, bei der jeder Knoten die Transaktionsdaten redundant speichert. Die Teilnehmer eines Blockchain-Netzwerks müssen sich weder kennen noch sich gegenseitig vertrauen und die protokolierten Transaktionen sind grundsätzlich transparent einsehbar. Außerdem benötigt eine Blockchain einen beispielsweise ökonomischen Unterbau, der Anreize für die Teilnehmer bietet, die notwendige Infrastruktur zu betreiben.

Das Projekt „Blockstack" nutzt das Blockchain-Netzwerk von Bitcoin, um Identitäten von Personen, Websites, Firmen etc. zu verwalten. Die auch im Bitcoin-Netzwerk verwendeten Adressen, die normalerweise nur Angaben zum Ort enthalten, an denen sich die Bitcoins befinden, werden mit weiteren Daten angereichert. Für das Bitcoin-Netzwerk sind alle Aktionen (beispielsweise die Weitergabe von Daten) nur Transaktionen von Bitcoins.

Im Paper „Decentralizing Privacy: Using Blockchain to Protect Personal Data" schlagen Zyskind, Nathan und Pentland vor, Zugriffsrechte in Bezug auf personenbezogene Daten in einer Blockchain zu halten. Die personenbezogenen Daten selbst werden dabei in einem separaten Speicher gehalten. Personenbezogene Daten werden symmetrisch mit einem zwischen betroffenen Personen und dem Dienst ausgehandelten geheimen Schlüssel verschlüsselt. Zugriffsrechte werden über Pseudonyme in die Blockchain geschrieben. Hierbei wird davon ausgegangen, dass Dienste „Honest

but curious“-Angreifer sind. Das heißt, sie verhalten sich ehrlich, folgen dem Protokoll, versuchen aber gleichzeitig möglichst viele sensible Daten zu erhalten.

6.2.4 Smart Contracts

Smart Contracts sind Programme, die Verträge in maschineninterpretierbarer Sprache repräsentieren sollen. Genauer gesagt handelt es sich dabei um eine Abfolge von Handlungsanweisungen an einen Computer, die die Vertragsvereinbarung technisch abbilden. Meist werden Smart Contracts in Verbindung mit ihrer Speicherung in einer Blockchain diskutiert. Durch die Unveränderlichkeit der in einer Blockchain gespeicherten Daten entsteht die Verbindlichkeit des „Vertrags“.

Die populärste Smart-Contracts-Plattform ist Ethereum mit der Kryptowährung „Ether“. Verträge werden mit der JavaScript-ähnlichen Sprache „Solidity“ formuliert. Ein Beispiel für die Nutzung von Ethereum ist Digix.[20] Von diesem Dienst wird Gold in Singapur eingelagert und für jedes Gramm ein Token in der Ethereum-Blockchain registriert. Anteile können grammweise gekauft und mit Bitcoins oder der Ethereum-eigenen Kryptowährung „Ether“ bezahlt werden. Die Tokens ermöglichen es, Besitzrechte an dem Gold in Sekundenschnelle weltweit zu übertragen.

In der Praxis ist die Ausdrucksmächtigkeit der maschineninterpretierbaren Vertragssprache zu beachten. Eine zu hohe Ausdrucksmächtigkeit lässt zwar viele Vertragsformen zu, birgt aufgrund der Komplexität jedoch die Gefahr des Missbrauchs von Ausdrücken und Sicherheitslücken. Eine zu geringe Ausdrucksmächtigkeit verhindert hingegen womöglich den Ausdruck gewünschter Inhalte von Smart Contracts.

Rechtlich ist zu beachten, dass ein Vertrag in der Regel zwei korrespondierende Willenserklärungen (Angebot und Annahme) voraussetzt. Es bleibt zu prüfen, inwieweit maschineninterpretierbarer Code, der in der Regel für Menschen nicht sehr verständlich ist, Willenserklärungen darstellen kann. Darüber hinaus gibt es Fälle, bei denen für Verträge die Schriftform vorgeschrieben ist.

6.2.5 Digitale Güter

Die Blockchain-Technologie eignet sich besonders zum Schutz digitaler Güter. Dabei geht es prinzipiell um jedes digitale Gut, das mit einem Nutzungsrecht versehen werden soll. Naheliegende Beispiele sind Musik- oder Bilddateien,[21] aber auch Tickets. Zusätzlich werden unter digitalen Gütern auch Komponenten des Internets of Things[22] verstanden.

Ziel des Einsatzes von Blockchains im Bereich digitaler Güter ist die Bestätigung des übertragenen Rechts zur Nutzung des Gutes durch die Verifikation der durchgeführten Nutzungsrechtetransaktion im Distributed Ledger der Blockchain.

Nachgelagert könnte die Umsetzung der Nutzungsrechte mit Nutzungskontrollmechanismen – beispielsweise dem IND²UCE Framework – unterstützt werden.

6.2.6 Probleme und Herausforderungen von Anwendungen mit Blockchains

Obwohl Anwendungen mit Blockchains noch nicht lange existieren, gab es bereits erfolgreiche Angriffe auf sie. Diese müssen bei der Konzeption von Anwendungen mit Blockchains beachtet werden.

6.2.6.1 Die Sybil-Attacke

Eine Sybil-Attacke ist ein Angriff auf Peer-to-Peer-Netzwerke. Sybil-Attacken sind dann möglich, wenn eine zentrale Authentifizierungs- oder Zertifizierungsinstanz nicht vorhanden ist. Durch die Erstellung vieler falscher Identitäten können beispielsweise Mehrheitsverhältnisse oder die Netzwerkorganisation manipuliert werden. Im Falle von Anwendungen mit Blockchains kann durch eine Sybil-Attacke das Netzwerk potenziell massiv verlangsamt werden.

6.2.6.1.1 Der DOS/STONED-Zwischenfall

Am 15.05.2014 wurde die Signatur des DOS/STONED-Virus in die Bitcoin-Blockchain eingefügt. Dies führte dazu, dass die Blockchain auf vielen Clients von Antivirensoftware gelöscht wurde. Laufende Bitcoin-Clients fingen daraufhin an, die gesamte Bitcoin-Blockchain (17 Gigabyte) erneut herunterzuladen. Kurz nach dem Vorfall hatte Microsoft eine Ausnahme für die Blockchain in ihre Antivirensoftware eingefügt. Prinzipiell könnte ein solcher Angriff dazu benutzt werden, kurzfristig die Mehrheitsverhältnisse im Netzwerk zu ändern, sodass diese für die Sicherheit der Blockchain notwendige Voraussetzung nicht mehr gilt.

Der DOS/STONED-Zwischenfall weist auf ein prinzipielles Problem hin: Einmal in eine Blockchain eingefügte Inhalte können nicht mehr gelöscht werden. Potenziell können auch illegale Inhalte in eine Blockchain eingefügt werden.[23] Die Betreiber der Netzwerkknoten würden sich dann strafbar machen.

6.2.6.1.2 Der DAO-Hack

DAO (Dezentrale Autonome Organisation) ist ein Unternehmen, das nur in Form von Smart Contracts (vgl. Abschnitt 4.2.2) in der Ethereum-Blockchain (vgl. Abschnitt 4.2.1) existiert. DAO hatte in einer Crowdfunding-Aktion über 160 Millionen US-Dollar in der Kryptowährung „Ether“ des Ethereum-Netzwerks eingesammelt.[24]

Mitte 2016 gelang es Angreifern, eine Schwachstelle im DAO-Code auszunutzen und ca. 3,6 Millionen Ether zu stehlen. Als dies bemerkt wurde, sank der Ether-Kurs von 21 auf 12 US-Dollar. Mittlerweile wurden die entsprechenden Transaktionen mittels eines so genannten Hard Forks rückgängig gemacht. Was in der Community als Erfolg gefeiert wird, ist aus Sicht der IT-Sicherheit das Außerkraftsetzen der Fälschungssicherheit der Blockchain durch eine Kollaboration von über 50 Prozent der Teilnehmer des Netzwerkes.

6.3 Digitale Identifikations- und Authentifikationssysteme

6.3.1 OpenID

OpenID[25] ist ein dezentrales Authentifizierungsprotokoll für Internet-Dienstanbieter. Es erlaubt einem Benutzer, der sich bei einem OpenID-Provider angemeldet hat, sich nun bei allen das System unterstützenden und diesem Provider vertrauenden Websites ohne erneute Authentifizierung anzumelden. Ein OpenID-Provider fungiert dabei jedoch nicht als Passwortmanager, da die üblichen Passwörter für einzelne Anwendungen entfallen. Der Benutzer authentifiziert sich schlichtweg ausschließlich gegenüber dem genutzten OpenID-Provider, der wiederum die sensiblen Daten des Nutzers sicher verwahrt. Ein Benutzer muss so nicht bei jeder Anwendung erneut personenbezogene Daten von sich preisgeben, um sich anmelden und eine neue Anwendung nutzen zu können.

Als Authentifizierungsmerkmal gegenüber diesen Websites dient eine so genannte OpenID, die von dem OpenID-Provider generiert wird. Durch die dezentrale Konzeption von OpenID und die freie Verfügbarkeit der benötigten Software kann jeder selbst zum OpenID-Provider werden. Bekannte Firmen, wie beispielsweise Yahoo, treten als OpenID-Provider auf und ermöglichen es anderen Websites, die von Yahoo generierte OpenID als Authentifizierungsmerkmal zu verwenden.

OpenID schreibt nicht vor, wie die Authentifizierung bei dem OpenID-Provider zu erfolgen hat. Neben dem Benutzernamen und dem Passwort kommen auch alternative Authentifizierungsverfahren, wie beispielsweise Tokens oder SmartCards, in Frage. Auch die Authentifizierung mit dem neuen Personalausweis ist prinzipiell möglich.

Bekannte Beispiele für OpenID-Provider sind Google oder Yahoo. Auf vielen Seiten erhält man bei der Registrierung die Möglichkeit, sich beispielsweise über

einen bereits vorhandenen Google-Account (Google-Konto) anzumelden.

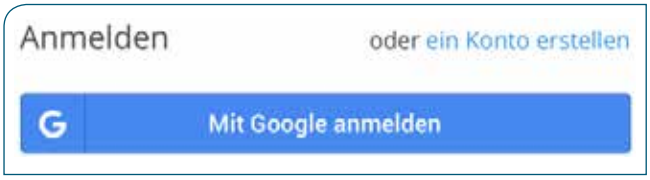

Abbildung 8: Möglichkeiten der Anmeldung (Beispiel: Dropbox.com)

Diese Art der Authentifizierung erleichtert in der täglichen Praxis das Arbeiten mit verschiedenen Anwendungen, bei denen sich der Benutzer sonst jeweils einzeln registrieren müsste. Bei einzelner Registrierung müssten dann auch jeweils pro Anwendung ein eigenständiger Benutzername und ein Passwort gewählt werden, um die Sicherheit der personenbezogenen Daten zu gewährleisten.

Mit seiner OpenID – seiner Identität – kann der Benutzer alle Anwendungen ohne erneute Registrierung nutzen, wenn die Anwendungen diese Art der Authentifizierung unterstützen. Die Anwendungen erfragen beim OpenID-Provider nur die Identität des Nutzers („Wer ist diese Person?“). Der Benutzer selbst muss sich nur gegenüber dem OpenID-Provider authentifizieren. Dieser sendet zur Verifizierung der Identität lediglich eine Benutzerkennung an die Anwendung, mit der nicht auf den eigentlichen Benutzer-Account des Nutzers geschlossen werden kann. Sensible Daten, beispielsweise personenbezogene Daten oder Passwörter, werden nicht übermittelt.

Beispiel: Herr Muster möchte sich beim Webdienstleisterportal „Flickr“ einloggen und dabei einen bereits vorhandenen Yahoo-Account nutzen, um nicht erneut den Registrierungsprozess durchlaufen zu müssen. Es öffnet sich eine Seite von Yahoo, auf der Herr Muster sich authentifiziert. Yahoo erkennt Herrn Muster und sendet Flickr anschließend eine Benutzerkennung, von der Flickr jedoch nicht explizit auf den betreffenden Yahoo-Nutzer schließen kann. Herr Muster ist danach bei Flickr angemeldet und kann den Dienst nutzen.

6.3.2 OAuth

Der Autorisierungsdienst „OAuth“ bietet einem registrierten Nutzer die Möglichkeit der Kontrolle über die Art und den Umfang der vom ihm erteilten Freigaben. Das Grundprinzip ähnelt der bereits beschriebenen OpenID, unterscheidet sich jedoch durch die Autorisierungsfunktion. Mittels OAuth kann der Benutzer Drittanwendungen auf einem sicheren und für den Nutzer kontrollierbaren Weg erlauben, auf seine bei einem OAuth-Provider hinterlegten Daten zuzugreifen. Den Zugriff auf die hinterlegten Daten kann der Benutzer selbst steuern. Einer Anwendung kann auch im Nachhinein die vorher genehmigte Nutzung bestimmter Daten wieder entzogen werden.

Ist beispielsweise bereits vor der ersten zu erteilenden Autorisierung bekannt, dass nur ein einmaliger Zugriff der Anwendung auf bestimmte Daten des Benutzers erfolgen darf, werden automatisch und ohne weitere Überwachung durch den Nutzer nach einmaliger Datenabfrage alle weiteren Abfragen verweigert. Diese Funktion kann mit einer mobilen TAN beim Onlinebanking verglichen werden, die nur für die einmalige Verwendung nach Anforderung genutzt werden kann und danach ihre Gültigkeit verliert.

OAuth kann nicht nur für die Nutzung sozialer Medien verwendet werden, sondern auch zur Vereinfachung des Online-Shoppings. Dies geschieht, indem Bankdaten beim OAuth-Provider hinterlegt werden, die der Benutzer während des Einkaufs mit der jeweiligen Website verknüpfen kann, bei der er eine Zahlung veranlassen möchte. Auch dabei erhält die Anwendung keine Kenntnis über Passwörter oder sonstige Anmeldedaten.

Beispiel: Herr Muster möchte die Fotos von seinem Skiurlaub mit Freunden über ein Flickr-Album teilen. Er meldet sich bei Flickr mit seinen dort bereits vor-

handenen Benutzerdaten an. Er nutzt anschließend die Option zur Freigabe von Daten unter Nutzung eines OAuth-Providers und authentifiziert sich bei diesem. Der Benutzer kann anschließend wählen, welche Angaben oder Daten Flickr (in diesem Fall bei Yahoo hinterlegte Fotos) nutzen soll, und erteilt die Erlaubnis zum Zugriff. Der OAuth-Provider erstellt daraufhin ein Zugriffstoken für die gewählten Benutzerdaten in seiner Datenbank und übermittelt diesen an Flickr. Flickr kann nun mit Hilfe des Zugriffstokens ausschließlich auf die spezifizierten Daten zugreifen.

6.3.3 OpenID Connect

OpenID Connect schließt für den Anwender die Lücke zwischen den bereits beschriebenen Diensten OpenID und OAuth. Mit diesen Diensten hat der Benutzer nur die Möglichkeit, sich entweder gegenüber einer gewünschten Anwendung zu authentifizieren (OpenID) oder einer Anwendung Zugriffsrechte auf Daten einzuräumen, die er bei seinem OAuth-Provider hinterlegt hat (OAuth) – nicht jedoch beides zugleich. OpenID Connect bietet beide Optionen in Kombination durch einen einzelnen OpenID-Connect-Provider.

Entstanden ist OpenID Connect als logische Folge der Weiterentwicklung von OAuth zu OAuth 2.0 und der ersten Überlegungen, welchen ID-Provider man einbinden könnte, um die fehlende Authentifizierungsmöglichkeit zu unterstützen, die die bisherigen Nutzungsmöglichkeiten von OpenID limitierte.

Viele der früheren OpenID-Provider, deren Dienstleistungen auch von einem durch ihre Nutzer autorisierten Zugriff auf Daten profitieren, nutzen mittlerweile OpenID Connect und sind daher OpenID-Connect-Provider. Es existieren mittlerweile auch firmeneigene Implementierungen von OpenID Connect, wie z. B. Facebooks „Facebook Connect“.

Beispiel: Herr Muster möchte die Fotos von seinem Skiurlaub mit Freunden über ein Flickr-Album teilen. Er möchte sich dazu bei Flickr mit seinem bereits vorhandenen OpenID-Connect-Account bei Yahoo anmelden, um nicht erneut den Registrierungsprozess bei Flickr zu durchlaufen. Es öffnet sich eine Seite von Yahoo, auf der Herr Muster sich authentifiziert. Yahoo erkennt Herrn Muster und sendet Flickr eine Benutzerkennung, von der Flickr jedoch nicht explizit auf den betreffenden Yahoo-Nutzer schließen kann. Herr Muster ist danach bei Flickr angemeldet und kann den Dienst nutzen. Der Benutzer kann anschließend wählen, welche Angaben oder Daten Flickr (in diesem Fall bei Yahoo hinterlegte Fotos) nutzen soll, und erteilt die Erlaubnis zum Zugriff. Yahoo erstellt daraufhin ein Zugriffstoken für die gewählten Benutzerdaten in seiner Datenbank und übermittelt dieses an Flickr. Flickr kann nun mit Hilfe des Zugriffstokens ausschließlich auf die spezifizierten Daten zugreifen.

OpenID bzw. OAuth wird u. a. von den folgenden Unternehmen unterstützt: Google, Facebook, Amazon, Xing, LinkedIn, Microsoft, Yahoo, Twitter, Strato, Hasso-Plattner-Institut, France Connect.

6.3.4 SAML

SAML (Security Assertion Markup Language, mittlerweile „SAML 2.0“) ist ein XML-Standard, der Sicherheits-Tokens verwendet, und ein offizieller OASIS-Standard (Organization for the Advancement of Structured Information Standards). Sicherheitsbezogene Informationen können mit ihm beschrieben und übertragen werden. SAML ermöglicht sowohl Autorisierung als auch Authentifizierung. Eine SAML-XML enthält dabei drei Beschreibungen: Details zur Authentifizierung selbst (beispielsweise Zeitpunkt, Ausführender, Art des Authentifizierungsmechanismus), Details zur Person selbst (beispielsweise Abteilungszugehörigkeit eines Angestellten innerhalb einer Firma) und Angaben darüber, ob diese Person die Berechtigung für die betroffenen Ressourcen hat.

Eingesetzt wird es beispielsweise von Google (bietet

Entwicklern eine Referenz-Implementierung zur Realisierung des SSO-Mechanismus an), Pan-European Proxy Service (PEPS), Microsoft (ADFS 2.0), McAfee (Cloud Identity Manager), Intel (Intel Cloud SSO), SAP (Netweaver App Server) und Oracle (Oracle Identity Federation).

6.3.5 Shibboleth

Shibboleth ist ein Open-Source-Projekt für verteiltes Single Sign-on (SSO) und Autorisierungen. Es basiert auf der Erweiterung von SAML und wird vor allem im wissenschaftlichen Bereich genutzt. In Deutschland wurde es durch organisatorischen und technischen Support des DFN und der Albert-Ludwigs-Universität Freiburg als „DFN-AAI“ (nationaler Zusammenschluss) realisiert. Weiterhin existieren jeweils nationale Föderationen wie „SWITCHaai“ (Schweiz) oder „HAKA“ (Finnland). Die Software besteht dabei aus drei Teilen: dem Identity-Provider, dem Service-Provider und dem Lokalisierungsdienst (optional).

Eingesetzt wird Shibboleth beispielsweise bei GigaMove (Datenaustausch über die RWTH Aachen), beim TextGrid-Verbundprojekt (Digitale Forschungsumgebung für Geisteswissenschaften) und WebConf (Webkonferenz-System des Deutschen Forschungsnetzes) sowie u. a. bei diversen Universitäten (TU Berlin, HU Berlin, Universität Tübingen, Universität Potsdam und anderen).

6.3.6 CAS (Central Authentication Service)

CAS wurde ursprünglich von der Universität Yale entwickelt und soll Universitäten und andere Bildungsinstitute vernetzen. Es ist ein offenes Protokoll und dient vor allem Bildungseinrichtungen zum Austausch von Wissen und Technologien. Login, Validierung und Logout werden über URLs realisiert. Die Anmeldung und Authentifizierung erfolgen über eine zentrale Instanz (Central Authenticate Server). Die Funktionsweise von CAS ist mit der von Shibboleth vergleichbar.

6.3.7 France Connect

France Connect[26] ist ein frankreichweites Netzwerk. Es erlaubt Bürgern, Behörden und Unternehmen den Onlinezugang zu und die Nutzung von öffentlichen Diensten in Frankreich, um administrative Prozesse zu beschleunigen und zu vereinfachen. Der Bürger kann sich hierbei ausweisen und Behörden autorisieren. France Connect basiert auf OpenID und OAuth 2.0.

6.4 Datennutzungskontrolle mit IND²UCE

Der Fokus von ISÆN liegt auf der Protokollierung von Datenschutzeinwilligungen und der Unterstützung des Austauschs personenbezogener Daten. Eine Überprüfung, ob personenbezogene Daten nur gemäß vorhandener Legitimationsgrundlagen verwendet werden, findet nicht statt. Mechanismen zur Datennutzungskontrolle können Unternehmen dabei unterstützen, versehentliche nicht erlaubte Datenverarbeitung zu vermeiden. Im Folgenden wird das IND²UCE Framework, eine Implementierung von Datennutzungskontrollmechanismen, beschrieben.

6.4.1 IND²UCE Framework

Das am Fraunhofer IESE entwickelte Sicherheitsframework „ IND²UCE “ (Integrated Distributed Data Usage Control Enforcement) macht die Grundprinzipien der Datennutzungskontrolle für die praktische Anwendung nutzbar.

Um dies zu erreichen, werden die klassischen Mechanismen der Zugriffskontrolle ergänzt bzw. erweitert, sodass die spezifische Nutzung von Daten jederzeit erkennbar und so letztlich auch kontrollierbar wird.

Ein wesentlicher Aspekt ist der kontrollierte Eingriff in Datenströme, um die Verwendung der Daten abhängig von der Nutzungssituation erfassen und steuern zu können. So müssen beispielsweise bestimmte Datenfelder je nach Adressat oder situativem Kontext ein- oder ausgeblendet werden.

Ein anderer wichtiger Aspekt ist das Nachverfolgen (Tracking) von Informationsflüssen, also die Fähigkeit zu erkennen, ob und über welche Wege bestimmte Daten durch das System fließen. Liegen entsprechende Trackinginformationen vor, besteht die Möglichkeit, durch entsprechend formulierte Richtlinien (Policys) differenziert Vorgaben in Bezug auf die Zulässigkeit von Datenflüssen und Datenflusswegen zu spezifizieren und deren Einhaltung zu überprüfen. Sofern diese Information unabhängig von Format und Darstellungsform unmittelbar und unauslöschlich mit den zu verfolgenden Daten verknüpft werden kann, lassen sich alle Repräsentationen und Kopien eines Datensatzes gegen unberechtigte Verwendung schützen.

Das dynamische Laufzeitverhalten des Frameworks und dessen komponentenbasierter Ansatz erlauben eine einfache Integration der Datennutzungskontrolle

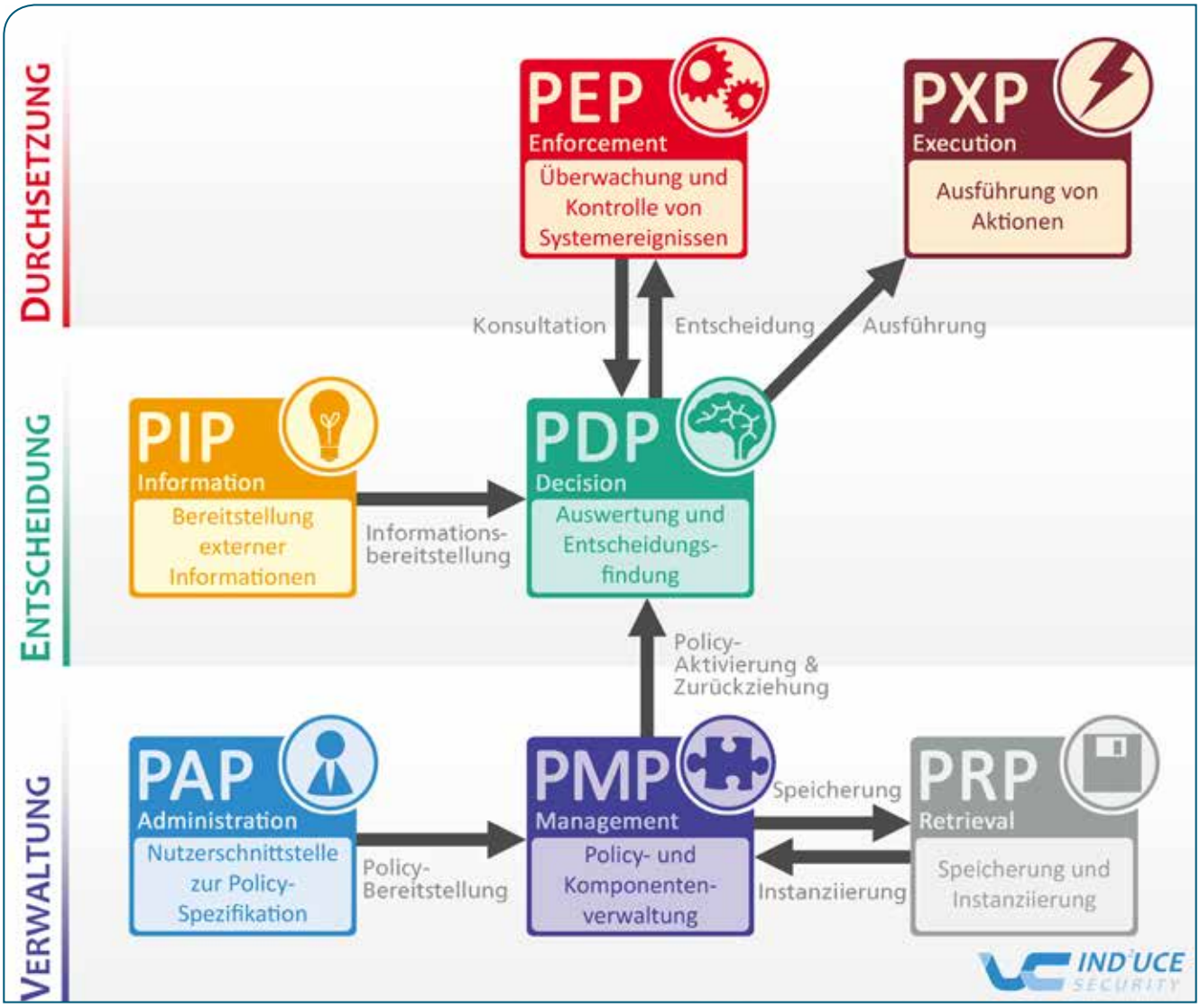

Abbildung 9: Architektur des IND²UCE Frameworks

in existierende System- und Softwarelandschaften. Die grundlegende Architektur des komponentenbasierten Frameworks IND²UCE zeigt Abbildung 9. Das Framework ist in die drei Ebenen „Manage", „Decide" und „Enforce" untergliedert, welche die Kernfunktionalität zur Durchsetzung von Datennutzungskontrollen erbringen.

6.4.1.1 Verwaltungsebene

Policy Administration Point (PAP)

Der PAP realisiert die einzige direkte Interaktionsschnittstelle zwischen Nutzer und System. Seine elementare Funktion besteht darin, eine benutzerfreundliche Schnittstelle anzubieten, über die sich Sicherheitsrichtlinien (Vorgaben zur zulässigen Datenverwendung) einfach und flexibel spezifizieren und verwalten lassen. PAPs müssen an den Wissensstand der Endanwender und die Sicherheitsbedürfnisse der Anwendungsdomäne angepasst werden. Einmal spezifizierte Sicherheitsrichtlinien
werden durch einen abschließenden Übersetzungsprozess in eine maschinenlesbare Form überführt.

Policy Management Point (PMP)

Hauptaufgabe des PMP sind die Organisation und Verwaltung der spezifizierten Sicherheitsrichtlinien. Dazu gehören das Aushandeln, Aktivieren, Modifizieren und Zurückziehen von Sicherheitsrichtlinien. Da das Framework als verteiltes und dynamisch sich änderndes System konzipiert ist, übernimmt der PMP zudem die zentrale Verwaltung und Kontrolle der während der Laufzeit erzeugten Komponenteninstanzen. Jede einzelne Systemkomponente muss sich also beim PMP vorab in geeigneter Weise mit Funktion und Schnittstellenbeschreibung registrieren.

Policy Retrieval Point (PRP)

Der Policy Retrieval Point (PRP) realisiert einen zuverlässigen Speicher zur langfristigen Aufbewahrung von Sicherheitsrichtlinien. Die einzige Komponente mit Zugriff auf diesen Speicher ist der PMP.

6.4.1.2 Entscheidungsebene

Policy Decision Point (PDP)

Im Zentrum des Frameworks steht die generische und technologieunabhängige Entscheidungskomponente PDP, die anhand von Sicherheitsrichtlinien über die Zulässigkeit von sicherheitsrelevanten Ereignissen wie z. B. Datenoperationen entscheidet. Diese Sicherheitsrichtlinien basieren auf dem Event-Condition-Action-Paradigma und erlauben die Verwendung der Obligation Specification Language (OSL). Mit Hilfe von OSL können Verbindlichkeiten (englisch „Obligation") spezifiziert werden (beispielsweise „Personenbezogene Daten müssen innerhalb von 14 Tagen gelöscht werden" oder „Ohne Genehmigung des Vorgesetzten dürfen nur zehn Akten pro Stunde geöffnet werden").

Policy Information Point (PIP)

Der PIP stellt zusätzliche Informationen bereit, die für die Entscheidungsfindung im PDP benötigt werden und im Systemereignis nicht vorliegen. Zusätzliche Informationen können Daten über Informationsflüsse oder kontextabhängige Daten, wie etwa die aktuelle Location oder WiFi-Konnektivität eines Endgeräts, sein. Kontextsensitivität erlaubt es, Sicherheitsmechanismen nur dann anzuwenden, wenn diese in der Situation angebracht sind. Dies ermöglicht beispielsweise allgemeine Verbote aufzulockern, zu denen Unternehmen sonst gezwungen sind. Aus dem allgemeinen Verbot „Smartphones sind im Unternehmen verboten, da Fotos von geheimen Informationen gemacht werden könnten" kann eine kontextsensitive Sicherheitsrichtlinie entstehen, wie z. B. „Fotos, die mit einem Smartphone innerhalb des Unternehmens aufgenommen wurden, dürfen auch nur dort angesehen werden".

6.4.1.3 Durchsetzungsebene

Policy Enforcement Point (PEP)

PEPs sind Kontrollkomponenten, die in bestehende Systeme integriert werden, um auf Informationsflüsse gemäß den spezifizierten Sicherheitsrichtlinien einzuwirken. PEPs erkennen und erfassen relevante Ereig-

nisse auf verschiedenen Systemebenen und können sie je nach Sicherheitsvorgabe zulassen, modifizieren oder verwerfen. Hierbei lassen sich Modifikationen wie z. B. Anonymisierungen oder Aggregationen von Daten sehr feingranular und situationsbedingt steuern. PEPs sind technologieabhängige Komponenten, da sie auf das jeweilige System angepasst werden müssen.

Policy Execution Point (PXP)
PXPs können zusätzliche Aktionen wie das Löschen von Daten, das Protokollieren von Operationen oder das Versenden von Benachrichtigungen durchführen.

Die Minimalkonfiguration des IND²UCE Frameworks zur Durchsetzung von Sicherheitsrichtlinien erfordert einen PDP für die Entscheidungsfindung und einen PEP zum Durchsetzen der Entscheidung.

6.4.2 Berücksichtigung von Informationsflüssen

In IND²UCE wird bei androidbasierten Laufzeitumgebungen das System „TaintDroid“ eingesetzt, um spezifische Datenflüsse während der Verarbeitung zu berücksichtigen. TaintDroid arbeitet dabei mit „Marken“ – genannt „Taint Tags“ –, die den relevanten Daten oder Datenquellen als permanente Attribute hinzugefügt werden. Die Marken haften sozusagen an den Daten und werden bei jedem Kopiervorgang unverändert übernommen. Durch diese Markierung lassen sich sowohl Datenflüsse erkennen als auch die Datenverwendung unabhängig von einer spezifischen Repräsentation berücksichtigen. Dadurch wird es beispielsweise möglich, Bildaufnahmen, die aufgrund des situativen Kontextes vertraulich zu behandeln sind (Foto auf Firmengelände o. Ä.), mit einer besonderen Markierung X zu versehen, die letztlich hilft zu verhindern, dass bestimmte Anwendungen diese Bilder unberechtigterweise verwenden. Da die Markierung den Bildern unauslöschlich anhaftet, kann eine entsprechende Richtlinie nicht nur für die Originalaufnahmen, sondern auch für alle künftigen Kopien formuliert werden. Eine spezifische Vorgabe wie z. B. „Picture DSC00123.jpg cannot be used by email“ lässt sich auf diese Weise eleganter und allgemeiner fassen zu „Any picture with taint tag X cannot be used by email“.

7 Bewertung von ISÆN

Das ISÆN-Konzept verknüpft zum einen die Möglichkeit, Verbraucher zu identifizieren. Zum anderen soll die Protokollierung von erteilten Datenschutzeinwilligungen in einer Blockchain eine bessere Nachvollziehbarkeit von getätigten Transaktionen ermöglichen. Hierdurch könnten Verantwortliche ihren datenschutzrechtlichen Dokumentations- und Informationspflichten nach der DSGVO unter Umständen besser nachkommen.

7.1 ISÆN-Identifier

7.1.1 Bewertung des ISÆN-Identifiers

Das ISÆN-Konzept ist ein Vorschlag für ein System, mit dem betroffene Personen nachvollziehen können, wer welche ihrer personenbezogenen Daten verarbeitet. Kern des Konzepts ist der ISÆN-Identifier, der als eindeutiges unveränderliches Identifikationsmerkmal (ID) zur Kennzeichnung der Daten einer natürlichen Person herangezogen werden soll. Die Idee besteht im Wesentlichen darin, die Existenz sowie den Transfer personenbezogener Daten jederzeit und überall durch Assoziation bzw. Abgleich mit der individuellen eindeutigen Identifikationsnummer erkenn- und nachvollziehbar zu machen.

Es ist anzunehmen, dass sich die elementaren personenbezogenen Bestandteile der ISÆN bei vielen Dienstleistungsanbietern bereits heute in deren Datenbeständen in der einen oder anderen Form finden lassen. So dürfte eine partielle automatisierte Rekonstruktion des ISÆN-Identifiers mit Hilfe von spezifisch angepassten Such- und Abgleichalgorithmen über die Datenbestände ohne größeren Aufwand machbar sein. Anhand der vielfältigen expliziten und strukturellen Querbezüge zwischen den Einzeldaten dürften so insbesondere auch die nachträgliche Einordnung und Identifizierung personenbezogener Informationen prinzipiell möglich sein. Dies könnte es Betreibern von Big-Data-Anwendungen erleichtern, betroffene Personen zu identifizieren und damit ihren datenschutzrechtlichen Pflichten nachzukommen.

Das ISÆN-Konzept sieht die Speicherung von Änderungen von eingegebenen personenbezogenen Daten, der Anfragen von Dienstanbietern und der entsprechenden Autorisierung zur Speicherung der Verarbeitung von Daten vor.

Im beschriebenen Anwendungsfall wird hierzu ein Hash des ISÆN-Identifiers (im Folgenden „ISÆN-Hash“ genannt) an den Dienstanbieter übermittelt und mit der Autorisierung zur Speicherung der Verarbeitung von Daten in der Blockchain gespeichert. Mit den in der Blockchain gespeicherten Informationen sollen Betroffene die Möglichkeit erhalten, jederzeit nachzuvollziehen, wem sie welche Einwilligungen zur Verwendung ihrer personenbezogenen Daten gegeben haben. Für den Dienstanbieter sowie weitere Akteure, die die Zuordnung des ISÆN-Hash zur betroffenen Person kennen (beispielsweise andere Dienstanbieter, die die betroffene Person bereits in Anspruch genommen hat), kann der ISÆN-Hash als personenbezogenes Datum gewertet werden. Die daraus resultierenden rechtlichen Implikationen und Anforderungen hinsichtlich technischer Ausgestaltungen, beispielsweise der Notwendigkeit einer derartigen Speicherung der Daten in der Blockchain, sodass sie jeweils nur für die betroffene Person und den Verantwortlichen einsehbar sind, werden nachfolgend (vgl. Abschnitt 7.2.2.1) genauer erläutert.

Rechtlich ist darüber hinaus zu klären, inwieweit der Händler als Verantwortlicher den (für ihn) personenbezogenen ISÆN-Hash an die Blockchain übermitteln darf. Falls nötig, könnte dies beispielsweise mittels einer entsprechenden Einwilligung legitimiert werden.

Konkrete Umsetzungen, Anpassungen oder Erweiterungen des ISÆN-Konzepts, die sowohl Transparenz und Nachvollziehbarkeit für betroffene Personen und Verantwortliche bieten als auch die aus der DSGVO hervorgehenden Anforderungen erfüllen, sollten in einem Projekt mit den französischen Partnern weiter ausgestaltet werden.

7.1.2 Identifizierungsmöglichkeit des ISÆN-Identifiers
Der ISÆN-Identifier könnte grundsätzlich als elektronisches Identifizierungsmittel nach der eIDAS-Verordnung ausgestaltet werden, sodass er auch in Deutschland als Identifizierungsmittel anzuerkennen wäre, wenn er im Rahmen eines elektronischen Identifizierungssystems ausgestellt ist, das bei der Kommission notifiziert und nach Art. 9 Abs. 2 im Amtsblatt der europäischen Union veröffentlicht wurde.

Elektronische Identifizierungsmittel sind gemäß Art. 3 Abs. 2 (EU) Nr. 910/2014 eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird. Ein elektronisches Identifizierungssystem wiederum ist nach Art. 3 Abs. 3 (EU) Nr. 910/2014 ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden. Um eine Anerkennungspflicht auszulösen, müsste die Verwendung des Identifiers, d. h. eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und mit einer Authentifizierung für den Zugang zu einem von einer öffentlichen Stelle in Deutschland erbrachten Online-Dienst nach deutschem Recht oder aufgrund der Verwaltungspraxis erforderlich sein, sodass ein in einem anderen Mitgliedsstaat ausgestelltes elektronisches Identifizierungsmittel (der französische ISÆN-Identifier) im ersten Mitgliedsstaat (Deutschland) für die Zwecke der grenzüberschreitenden Authentifizierung für diesen Online-Dienst anerkannt werden kann. Aufgrund der Tatsache, dass das gewählte Anwendungsbeispiel im Privatsektor verankert ist, scheint für derartige Transaktionen keine Identifizierungsnotwendigkeit vorgeschrieben zu sein. Gleichwohl wird gemäß EWG 17 der eIDAS-Verordnung der Privatsektor ermutigt „freiwillig elektronische Identifizierungsmittel im Rahmen eines notifizierten Systems zu Identifizierungszwecken zu verwenden, wenn dies für Online-Dienste oder elektronische Transaktionen nötig ist“. So könnte sich der Privatsektor „auf eine elektronische Identifizierung und Authentifizierung stützen, die in vielen Mitgliedsstaaten zumindest bei öffentlichen Diensten schon weit verbreitet ist“, um Unternehmen und Bürgern den grenzüberschreitenden Zugang zu ihren Online-Diensten zu erleichtern.

Insofern müsste sich der ISÆN-Identifier als eine Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird, einstufen lassen und zusätzlich von einem elektronischen Identifizierungssystem ausgestellt werden. Das Identifizierungssystem müsste in diesem Zusammenhang ein entsprechendes Sicherheitsniveau aufweisen.

Daher erscheint es sachgerecht, auch für Online-Dienste, die keinen hoheitlichen Bezug aufweisen, Identifizierungsmittel anzubieten bzw. auf solche zurückzugreifen, die im öffentlichen Sektor bereits bestehen. Zu bedenken ist jedoch, dass der ISÆN-Identifier als elektronisches Identifizierungsmittel zumindest gemäß Art. 7 lit. b im notifizierenden Mitgliedsstaat für den Zugang zu mindestens einem Dienst verwendet werden muss, der von einer öffentlichen Stelle bereitgestellt wird und für den eine elektronische Identifizierung erforderlich ist. Dies sollte bei der näheren Ausgestaltung des ISÆN-Identifiers berücksichtigt werden, wobei klärungsbedürftig ist, ob eine Softwareapplikation in diesem Zusammenhang als elektronisches ausstellendes Identifizierungssystem geeignet bleibt und das erforderliche Sicherheitsniveau aufweisen kann.

Zusammenfassend zeigt sich, dass die Erfüllung der Anforderungen aus der eIDAS-Verordnung eine Anerkennungspflicht in weiteren Mitgliedsstaaten bedingen würde. Auch sollten im Privatsektor verstärkt elektronische Identifizierungsmittel eingesetzt werden, um das Vertrauen in elektronische Transaktionen zu stärken.

7.2 Datenschutzrechtliche Einordnung von ISÆN

Aus datenschutzrechtlicher Sicht gestaltet sich die rechtliche Einstufung des gewählten Anwendungsszenarios als äußerst komplex, da die verschiedenen Vorgänge (Daten in der App, Übermittlung der ID an Webshop-Betreiber, Speichern in der Blockchain, direktes Versenden der Daten an Webshop-Betreiber) dem Grunde nach selbst zunächst systematisch und isoliert voneinander zu betrachten wären. Gleichwohl zeigen sich aber erst durch die Betrachtung des Gesamtszenarios die rechtlich potenziell kritisch zu würdigenden Aspekte, da sich unter Umständen nachträglich weitere Identifizierungsmöglichkeiten ergeben, die so zu Anfang nicht vorlagen. Die rechtliche Untersuchung der einzelnen Teilvorgänge erfolgt damit in der Gesamtschau. Zunächst sollen vorab jedoch für ein besseres Verständnis einige grundlegende Definitionen aufgeführt sowie im Konkreten die Grundsätze der DSGVO aufgezeigt werden. Definitionen nach Art. 4 (EU) 2016/679:

- „personenbezogene Daten“ (Nr. 1): alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
- „Verarbeitung“ (Nr. 2): jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- „Pseudonymisierung“ (Nr. 5): die Verarbeitung personenbezogener Daten in einer Weise, durch die die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen sowie organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
- „Verantwortlicher“ (Nr. 7): die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedsstaaten vorgegeben, so kann der Verantwortliche bzw. können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten vorgesehen werden.
- „Dritter“ (Nr. 10): eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

7.2.1 Grundsätze der DSGVO

Die DSGVO regelt in Art. 5 (EU) 2016/679 eine Vielzahl von Grundsätzen für die Verarbeitung personenbezogener Daten, die der rechtlichen Bewertung zugrunde gelegt werden sollen. Diese müssen kumulativ vorliegen.[27]

7.2.1.1 Rechtmäßigkeit (lit. a)
Grundsätzlich steht die Verarbeitung personenbezogener Daten nach der DSGVO unter dem allgemeinen Grundsatz des so genannten Verbots mit Erlaubnisvorbehalt. Eine Datenverarbeitung ist demnach erst einmal verboten, sofern nicht eine normierte Ausnahme vorliegt.[28] Die Verarbeitung der Daten ist insoweit rechtmäßig, als die Voraussetzungen des Art. 6 (EU) 2016/679 erfüllt sind, d. h. eine Einwilligung vorliegt oder die Verarbeitung auf einer sonstigen zulässigen Rechtsgrundlage erfolgt. Letztere ist u. a. die Datenverarbeitung, die für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder für eine rechtliche Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist.[29]

7.2.1.2 Treu und Glauben (lit. a)
Die Verarbeitung nach Treu und Glauben war bereits in der Datenschutzrichtlinie enthalten und findet sich auch in Art. 8 Abs. 2 S. 1 GRCh. Der Grundsatz ist für die Auslegung verschiedener Begriffe wie des „berechtigten Interesses“ an einer Datenverarbeitung (Art. 6 Abs. 1 S. 1 lit. f (EU) 2016/679) oder „vernünftige Erwartungen“ (EWG 47 S. 1, 50 S. 6) hilfreich. Eine eigenständige Bedeutung ist jedoch darüber hinaus nicht zu erwarten.[30]

7.2.1.3 Transparenz (lit. a)
Der Grundsatz der Transparenz, der auch in Art. 12 Abs. 1 zum Ausdruck kommt, entspringt der Notwendigkeit, den Umgang mit personenbezogenen Daten für die betroffenen Personen transparent zu gestalten, damit diese in der Lage sind, selbstbestimmt über die Verwendung ihrer Daten zu bestimmen. Der Transparenzgedanke schlägt sich in verschiedenen in der DSGVO normierten Betroffenenrechten nieder. So stehen der betroffenen Person gegenüber den Verantwortlichen verschiedene Informations-, Benachrichtigungs- und Berichtigungsrechte zu (Art. 13 bis Art. 16). Darüber hinaus kann die betroffene Person unter bestimmten Voraussetzungen die Löschung ihrer Daten verlangen (Art. 17), z. B. wenn der Zweck, zu dem die Daten ursprünglich verarbeitet wurden, nicht mehr besteht oder die erteilte Einwilligung der betroffenen Person widerrufen wurde. Hat der Verantwortliche die Daten öffentlich gemacht, muss er im Falle, dass die betroffene Person ihr Löschrecht in Anspruch nimmt, auch die nachgeordnet verarbeitenden verantwortlichen Stellen über die Ausübung des Löschrechts informieren (Art. 17 Abs. 2).

7.2.1.4 Zweckbindung (lit. b)
Der Zweckbindungsgrundsatz sieht vor, dass Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Änderungen des Verarbeitungsprozesses sind nur erlaubt, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar sind (Art. 5 Abs. 1b und Art. 6 Abs. 4).

7.2.1.5 Datenminimierung (lit. c)
Nach der Datenminimierung steht die Verarbeitung personenbezogener Daten unter der Prämisse, dass sie „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ sollte (Art. 5 Abs. 1 c).[31] Um eine wirksame Umsetzung dieses Prinzips zu erreichen, wurde u. a. der „Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen“ in der DSGVO festgeschrieben (Art. 25). In Bezug auf die Technikgestaltung (Privacy by Design) sieht die DSGVO vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen muss, um die Datenschutzgrundsätze zu wahren. Dabei soll u. a. eine dem Stand der Technik entsprechende Datenverarbeitung gewährleistet werden.

7.2.1.6 Richtigkeit (lit. d)
Der Grundsatz der Richtigkeit wird in EWG 39 S. 11 (EU) 2016/679 näher erläutert. Danach sollen alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Der Grundsatz wird damit im Berich-

tigungsanspruch gemäß Art. 16 (EU) 2016/679 näher konkretisiert.

7.2.1.7 Speicherbegrenzung (lit. e)
Die Speicherbegrenzung schreibt vor, dass die Identifizierung der betroffenen Person nur so lange möglich sein soll, wie es für die Zwecke, für die sie verarbeitet wird, erforderlich ist.

7.2.1.8 Integrität und Vertraulichkeit (lit. f)
Das Prinzip der Datensicherheit ist in Art. 5 Abs. 1 lit. f verankert. Danach sollen Daten in einer Weise verarbeitet werden, die eine „angemessene Sicherheit der personenbezogenen Daten gewährleistet". Nach Art. 32 Abs. 1 treffen der Verantwortliche und der Auftragsverarbeiter „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten", „unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen".

7.2.1.8.1 Rechenschaftspflicht (Abs. 2)
Darüber hinaus wird in Art. 5 Abs. 2 (EU) 2016/679 eine so genannte Rechenschaftspflicht normiert, wonach der Verantwortliche nachweisen muss, dass er die Grundsätze eingehalten hat.

7.2.2 Sachlicher Anwendungsbereich
Nach Art. 2 Abs. 1 (EU) 2016/679 gilt die DSGVO „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen".

7.2.2.1 Personenbezogene Daten
In der Folge soll eine Untersuchung erfolgen, ob und falls ja welche Daten als personenbezogen einzustufen sind.

7.2.2.1.1 ISÆN-Identifier
Nach Art. 4 Nr. 1 sind „personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann". Von der Person, um deren personenbezogene Daten es sich handelt, wird in der DSGVO als von der „betroffenen Person" gesprochen.

Grundsätzlich ist anzumerken, dass auch Kennnummern, wie der ISÆN-Identifier, einen Personenbezug aufweisen können, wenn über sie eine Identifizierbarkeit der Person hergestellt werden kann (vgl. oben Art. 4 Nr. 1). Auch pseudonymisierte Daten können unter Umständen wie personenbezogene Daten zu behandeln sein. Erwägungsgrund 26 S. 2 besagt, dass „einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können, […] als Informationen über eine identifizierbare natürliche Person betrachtet werden" sollen. Eine Pseudonymisierung liegt nach Art. 4 Nr. 5 allerdings nur vor, „sofern die zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden". Die Grundsätze des Datenschutzes gelten hingegen nicht, wenn mit anonymen Daten umgegangen wird (siehe Erwägungsgrund 26 S. 5). Dies kann der Fall sein, wenn perso-

nenbezogene Daten so bearbeitet wurden, „dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“ (Erwägungsgrund 26 S. 5 HS 2). Der wesentliche Unterschied zwischen anonymen und pseudonymen Daten besteht darin, dass für Letztere eine Zuordnungsregel existiert, die die unter dem Pseudonym erfassten Daten den Identifikationsmerkmalen der Person zuweist. Bei der Betrachtung kommt es entscheidend darauf an, aus welcher Sicht der Personenbezug beurteilt wird. Für Stellen, die den besagten Zuordnungsschlüssel nicht kennen, sind pseudonymisierte Daten quasi anonym.[32] Gleichwohl wird in Erwägungsgrund 26 auch deutlich, dass der europäische Gesetzgeber die Frage, ob Daten einen Rückschluss auf eine identifizierte oder identifizierbare Person zulassen und demnach ein Personenbezug gegeben ist, von den dafür zur Verfügung stehenden Mitteln abhängig macht. Bei den Mitteln soll es sich um solche handeln, die „von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Person direkt oder indirekt zu identifizieren“ (Erwägungsgrund 26). Hierzu sind alle „objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand“ heranzuziehen, „wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklung zu berücksichtigen sind“ (Erwägungsgrund 26). Jüngst hat der EuGH[33] sich zum Personenbezug von IP-Adressen geäußert. Danach ist „eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung“, „wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen“.[33]

Im Falle des ISÆN-Identifiers ist ein direkter Rückschluss auf die personenbezogenen Daten möglich. Bereits Kenntnis darüber, wie die personenbezogenen Daten angeordnet sind, ermöglicht es, die Inhalte der personenbezogenen Daten zu kennen. Eine Pseudonymisierung liegt nicht vor, da die Daten selbst nicht durch ein Kennzeichen mit dem Zweck ersetzt werden, dass die Bestimmung der betroffenen Person ausgeschlossen oder erschwert wird. Insofern ist davon auszugehen, dass der ISÆN-Identifier selbst ein Kennzeichen ist, bzw. eine Zusammenfassung der verwendeten personenbezogenen Daten, deren Einzelangaben sich der Person zuordnen lassen.[34]

7.2.2.1.2 Daten in der Blockchain

Der aus den personenbezogenen Daten erzeugte Hash ist zwar eindeutig, lässt aber keinen unmittelbaren Rückschluss auf den Inhalt der personenbezogenen Daten des Nutzers zu. Der Hashwert selbst dürfte dem Grund nach als anonymes Datum zu werten sein. Grundsätzlich ist ein völliger Ausschluss einer Reidentifizierung aufgrund der heute zur Verfügung stehenden Informationstechnologien de facto selten gegeben.[35] In der Regel liegt eine „faktische“ Anonymität vor.[35] Dabei kommt es entscheidend darauf an, ob das Risiko einer Reidentifizierung vorliegt. Berücksichtigt werden müssen hierbei das vorhandene oder erwerbbare Zusatzwissen des Datenverwenders, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit.[36] Somit muss regelmäßig geprüft werden, ob erworbenes Zusatzwissen eine Identifizierbarkeit der ursprünglich anonymen Daten möglich macht. Sofern dies gegeben ist, unterliegen die Daten zu dem Zeitpunkt der DSGVO, sodass die Datenverarbeitung rechtswidrig ist, wenn entsprechende Vorgaben nicht eingehalten werden.[37]

Die in der Blockchain gespeicherten Informationen über die Transaktionen (Speicherung, Weitergabe, Löschung, ...) der Daten einer Person sind keine personenbezogenen Daten.

Ferner ist zu beachten, dass möglicherweise personenbezogene Daten eines weiteren Akteurs in der Blockchain gespeichert werden. Der weitere Akteur wäre in dem oben genannten Beispiel ein Webshop-Betreiber. In der Blockchain müssen – in verschlüsselter Form – Informationen beispielsweise darüber gespeichert werden, an wen die Daten weitergegeben wurden (beispielsweise an www.xyz.com). Die DSGVO findet allerdings keine Anwendung auf die Verarbeitung personenbezogener Daten juristischer Personen (siehe ErwG 14 S. 2), sondern lediglich auf die Verarbeitung personenbezogener Daten von natürlichen Personen. Juristische Personen sind Personenvereinigungen oder Zweckvermögen mit gesetzlich anerkannter rechtlicher Selbständigkeit.[38] Zivilrechtlich zählen hierzu u. a. Körperschaften des privaten Rechts, wie eingetragene Vereine, sowie Stiftungen, GmbHs, Aktiengesellschaften und Genossenschaften. In der Vergangenheit wurde in Bezug auf das Bundesdatenschutzgesetz allerdings auch die Ansicht vertreten, dass für den Fall, dass es sich bei Einzelangaben über Personengruppen, die auf ein bestimmtes oder bestimmbares Mitglied abzielen, dennoch um personenbezogene Daten handelt. Dies war beispielsweise für Daten über die finanzielle Situation einer Ein-Mann-GmbH der Fall.[39] Auch nach der Rechtsprechung des Europäischen Gerichtshofs wurde einer juristischen Person die Grundrechtsfähigkeit für das Datenschutzgrundrecht nach Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union zuerkannt.[40] In Erwägungsgrund 14 S. 2 der DSGVO werden jedoch explizit der Name, die Rechtsform und die Kontaktdaten der juristischen Person als solche Daten genannt, auf die die DSGVO keine Anwendung findet. Sofern sichergestellt ist, dass es sich bei dem Akteur (Webshop-Betreiber) um eine juristische Person und nicht etwa um eine natürliche Person handelt, und soweit auf der Blockchain lediglich die von der DSGVO genannten Daten (Name, Rechtsform und Kontaktdaten des Akteurs) gespeichert und an den Nutzer über ein sogenanntes Daten-GPS weitergegeben werden, bestehen datenschutzrechtlich keine Bedenken. Sollte es jedoch möglich sein, dass der genannte Akteur eben auch keine juristische Person sein könnte, weil er beispielsweise als Gesellschaft bürgerlichen Rechts (§ 705 BGB) organisiert oder eine natürliche Person ist, müssten die Grundsätze der DSGVO berücksichtigt werden.

7.2.2.1.3 Übermittelte Daten

Die an den Webshop-Betreiber von der betroffenen Person direkt übermittelten Daten sind unstreitig personenbezogene Daten. Diese sind für die Erfüllung der Verbindlichkeit aus dem Vertrag Kunde/Webshop-Betreiber erforderlich.

7.2.2.1.4 Potenziell zusammengesetzte Daten

Infolge des Erhalts der personenbezogenen Daten durch die betroffene Person hat der Webshop-Betreiber nunmehr die Möglichkeit, den in der Blockchain gespeicherten Hash mit den personenbezogenen Daten zu verknüpfen, sodass hierdurch eine direkte Zuordnung möglich ist. Sofern die Blockchain als öffentlicher, einsehbarer Speicher ausgestaltet ist, hat der Betreiber die Möglichkeit zu sehen, wem die identifizierte Person weitere Zugriffsrechte erteilt hat. Demnach kommt es in diesen Fällen auch nicht auf entsprechende (rechtliche) Mittel an, die zwecks Identifizierung herangezogen werden können, da der Betreiber von der betroffenen Person direkt die personenbezogenen Daten zugeschickt bekommt. Hierdurch kann er unweigerlich – sofern der Hash nicht für jede Transaktion bzw. für den Identifier jedes Mal neu erzeugt wird – eine Zuordnung vornehmen. Aus datenschutzrechtlicher Sicht ist es demnach erforderlich, die Daten in der Blockchain so zu speichern, dass sie jeweils nur für die betroffene Person und den Verantwortlichen einsehbar sind. Neben diesen technischen Möglichkeiten könnte auch für jede einzelne Transaktion ein entsprechendes neues Pseudonym verwendet werden, um das Risiko einer Identifizierung so gering wie möglich zu halten.

7.2.2.2 Verarbeitung
Eine Verarbeitung bezeichnet nach Art. 4 Nr. 2 „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch die Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung". Der frühere deutsche und unionsrechtliche Dreiklang aus Erheben, Verarbeiten und Nutzen, der unter dem Begriff der „Verarbeitung i. w. S." subsumiert wurde, ist so damit nicht mehr ersichtlich. Unter dem Begriff „Speichern" versteht man das Aufbewahren auf einem Datenträger zum Zwecke der weiteren Verarbeitung.[41]

7.2.2.3 Daten in der App
Die Daten werden unweigerlich in der App gespeichert und fallen demnach unter die Definition der Verarbeitung.

7.2.2.4 Daten in der Blockchain
In der Blockchain werden der Hash, Änderungen an den gespeicherten Daten in der Anwendung, Anfragen von Dienstanbietern sowie die Weitergabe der personenbezogenen Daten an diese gespeichert. Personenbezogene Daten des Anwenders werden zwar nicht in der Blockchain gespeichert, durch eine potenzielle Verknüpfung mit den versendeten Daten können sie jedoch zu solchen werden (siehe oben).

7.2.2.5 Daten beim Webshop-Betreiber
Eine Speicherung und weitere Verarbeitung der personenbezogenen Daten erfolgen im Nachgang durch den Webshop-Betreiber.

7.2.2.6 Einordnung der auftretenden Akteure
An dieser Stelle sollen die im skizzierten Anwendungsszenario auftretenden Akteure datenschutzrechtlich eingeordnet werden und ihre mit der jeweiligen Rolle entsprechend verbundenen Rechte und Pflichten aufgezeigt werden. Die DSGVO behält die bisherige Rollenklassifikation „betroffene Person", „Verantwortlicher", „Auftragsverarbeiter", „Dritte" bei.

Die betroffene Person ist dabei grundsätzlich diejenige, die geschützt werden soll. Der Schutz der sie betreffenden personenbezogenen Daten ist ein Grundrecht jeder natürlichen Person, Art. 7, 8 GRCh.[42] Der Verantwortliche hingegen ist der primäre Adressat der DSGVO, der entsprechend die Rechte und Pflichten bei der Verarbeitung personenbezogener Daten zu erfüllen hat. Mit der DSGVO können auch mehrere „Verantwortliche" gemeint sein, wenn sie gemeinsam über Zweck und Mittel der Verarbeitung entscheiden, siehe Art. 26 (EU) 2016/679. Auftragsverarbeiter werden im Rahmen der DSGVO vielfach selbst als Adressat datenschutzrechtlicher Pflichten neben dem Verantwortlichen vorgesehen. Gleichwohl sind sie weisungsgebunden und verarbeiten die personenbezogenen Daten im Auftrag des Verantwortlichen, sodass Letzterer über die Zwecke und Mittel entscheidet.[43] Dritte hingegen sind, abgesehen von potenziellen Haftungsansprüchen gegen Verantwortliche und Auftragsverarbeiter, vom Anwendungsbereich der DSGVO nicht erfasst.[44]

7.2.2.6.1 Anwender
Der Anwender der Ævatar-App ist gleichzeitig der Kunde des Webshop-Betreibers und als betroffene Person im datenschutzrechtlichen Sinne anzusehen.

7.2.2.6.2 Webshop-Betreiber/Dienstanbieter
Unstreitig ist der Webshop-Betreiber als Verantwortlicher anzusehen, da er die personenbezogenen Daten des Anwenders (betroffene Person) zwecks Erfüllung seiner vertraglichen Verpflichtung aus der Online-Transaktion verarbeitet. Verantwortliche können insoweit sowohl natürliche als auch juristische Personen sein, siehe Art. 4 Nr. 7 (EU) 2016/679.

7.2.2.6.3 Weitere Akteure
Hier müssen die Vorgänge des Anwendungsszenarios näher beleuchtet werden. Aufgrund der Tatsache, dass der Anwender unstreitig seine personenbezogenen Daten in der Ævatar-App speichert, können noch weitere Akteure auftreten, die entweder als Verantwortliche, Dritte, Empfänger oder gar als Auftragsverarbeiter anzusehen sind.

7.2.2.6.3.1 Daten in der App
Potenziell Verantwortliche könnten hierbei der App-Anbieter, der App-Entwickler, der Betriebssystem-Hersteller, der Geräteanbieter sein, sowie unter Umständen auch der Betreiber der Server-Infrastruktur, wenn die auf dem Smartphone gespeicherten Daten auf zentralen Servern beispielsweise zu Sicherungszwecken abgelegt werden.[45] Die Qualifizierung als Verantwortlicher setzt zumindest voraus, dass die personenbezogenen Daten von diesen Stellen entsprechend verarbeitet werden können, d. h. dass diese lokal und sicher derart gespeichert sind, dass lediglich der Anwender alleinigen Zugriff darauf hat. Aufgrund der Tatsache, dass der Sachverhalt hier wenig Aufschluss diesbezüglich gibt, soll auf weitere Ausführungen in diesem Zusammenhang verzichtet werden. Gleichwohl müsste, sofern die App selbst den Hash aus den personenbezogenen Daten erstellt, ein Zugriff durch den Anbieter/Entwickler der App vorgesehen sein, da diese dann den Wert in der App erzeugt, und insoweit nicht lokal und nicht in der alleinigen Sphäre des Anwenders. Die Artikel-29-Datenschutzgruppe hatte in ihrer Stellungnahme zu Apps auf intelligenten Endgeräten festgehalten, dass App-Entwickler in dem Umfang, in dem sie die Zwecke und Mittel der Verarbeitung personenbezogener Daten auf intelligenten Endgeräten festlegen, als für die Verarbeitung Verantwortliche im Sinne der Datenschutzrichtlinie anzusehen sind.[46]

7.2.2.6.3.2 Übermittlung des ISÆN-Hashs an Webshop-Betreiber
Weitere Akteure liegen nicht vor.

7.2.2.6.3.3 Speichern in der Blockchain
Werden in der ISÆN-Blockchain personenbezogene Daten gespeichert, könnten andere Teilnehmer des Blockchain-Netzwerks als Verantwortliche oder Dritte einzustufen sein. Das Blockchain-Konzept gestaltet sich als offenes, dezentrales System, das grundsätzlich für alle Teilnehmer einsehbar ist. Dabei speichert jeder einzelne Teilnehmer selbst eine lokale Kopie der Blockchain. Sofern es sich hierbei um personenbezogene Daten handelt, ist die Einordnung als Verantwortlicher für jeden einzelnen Teilnehmer grundsätzlich denkbar. Eine Auftragsdatenverarbeitung würde ausscheiden, da weder ein Auftrag geschlossen wird noch eine Weisungsgebundenheit zwischen Netzwerk-Teilnehmern gegeben ist (die Teilnehmer kennen sich unter Umständen nicht). Die dezentrale Ausgestaltung bezweckt in diesem Sinne gerade die autoritäre Funktion eines Einzelnen zu verhindern. In Abhängigkeit davon, ob sich eine Zuordnung nachträglich ermöglichen lässt, dürften die lokale Speicherung aller Daten und die Fähigkeit zur Identifikation dazu führen, dass die gespeicherten Daten schützenswert sind, sodass für den Teilnehmer, dem die Identifizierung möglich ist, die Pflicht besteht, die Grundsätze der DSGVO einzuhalten.

Rechtlich ist dabei zu klären, inwieweit der Dienstanbieter dann als Verantwortlicher den (für ihn) personenbezogenen ISÆN-Hash in der Blockchain weiter speichern darf, da dies unter Umständen als legitimierungsbedürftig (aufgrund einer potenziellen Übermittlung) zu werten wäre. Falls nötig, müsste mangels ersichtlicher gesetzlicher Rechtsgrundlagen mittels einer entsprechenden Einwilligung legitimiert werden.

7.2.2.6.3.4 Versenden der Daten an Webshop-Betreiber
Weitere Akteure, die in die bestehende Klassifizierung einzuordnen wären, bestehen nicht.

7.2.3 Zwischenergebnis
Zusammenfassend zeigt sich, dass die unterschiedlichen Vorgänge sowohl in ihrer Eigenständigkeit als

auch durch ihre Verknüpfung datenschutzrechtlich einzustufen sind, sodass an dieser Stelle die aus der DSGVO entstehenden Pflichten, die Verantwortliche zu erfüllen haben, aufgezeigt werden sollen. Hierbei wird lediglich auf die in diesem Szenario besonders relevanten Grundsätze und auf den Vorgang des Speicherns in der Blockchain abgestellt, wobei die nachträgliche Zuordnungsmöglichkeit berücksichtigt wird (siehe oben). Die beiden anderen Vorgänge, Speichern in der App sowie der Vorgang im Webshop, werden nicht durch das ISÆN-Konzept beeinflusst.

7.2.4 Erfüllung der Schutzprinzipien

Die zuvor identifizierten Verantwortlichen müssen die oben beschriebenen Grundsätze erfüllen. Wenn das ISÆN-Konzept so umgesetzt wird, dass eine nachträgliche Verknüpfung ausgeschlossen ist, bleibt es bei der Anonymität der Daten, sodass in diesen Fällen der Anwendungsbereich der DSGVO nicht gegeben ist.

Im in Abschnitt 3.1 beschriebenen Anwendungsszenario hat der Webshop-Betreiber aufgrund des Vertragsrechts eine Legitimation, die personenbezogenen Daten des Käufers zu verarbeiten. Er benötigt also keine Einwilligung des Betroffenen, um zur Vertragsabwicklung die personenbezogenen Daten des Käufers zu verarbeiten. Will der Webshop-Betreiber jedoch die personenbezogenen Daten des Käufers zusätzlich, beispielsweise zu Marketingzwecken, verwenden, könnte eine Einwilligung des Betroffenen notwendig werden. Darüber hinaus sind auch andere Anwendungsfälle denkbar, bei denen keine Legitimation zur Verarbeitung personenbezogener Daten aufgrund einer bestehenden Rechtsvorschrift besteht.

Alle zuvor identifizierten Verantwortlichen müssen demnach sicherstellen, dass die Verarbeitung aufgrund einer Einwilligung oder sonstigen Rechtsgrundlage erfolgt. Gleichzeitig muss die betroffene Person nachvollziehen können, ob und durch wen eine Datenverarbeitung erfolgt. Des Weiteren dürfen die Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Die Verantwortlichen müssen „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ ergreifen, „unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“, siehe Art. 32 Abs. 1 (EU) 2016/679. Die Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein.

Hier zeigt sich deutlich, dass die nachträgliche Identifizierung mit der Folge, dass ein Personenbezug zu dem Zeitpunkt gegeben ist, dazu führt, dass die Datenschutz-Grundsätze einzuhalten sind. Hierbei ist fraglich, ob es bereits eine Legitimation gibt. Da der Speicher der Blockchain ein zusätzliches Speichermedium ist, könnte grundsätzlich angenommen werden, dass die Daten tatsächlich zwecks Erfüllung des Vertrages mit dem Anwender auch in der Blockchain gespeichert werden. Eine Legitimation wäre demnach (noch) gegeben. Die Daten würden nach wie vor für den gleichen Zweck verwendet werden. Gleichwohl könnte das zusätzliche Speichern am Gebot der Datenminimierung scheitern. Die zusätzliche Speicherung in der Blockchain, deren Inhalt sich demnach für alle Teilnehmer, die eine Identifizierung vornehmen können, als ein solcher mit Personenbezug erweist, erscheint weder angemessen noch auf das für die Zwecke notwendige Maß beschränkt zu sein. Diese zusätzliche Speicherung ist demnach tatsächlich nicht notwendig, da sie für den Zweck der Verarbeitung nicht erforderlich ist. Gleichwohl ermöglicht die gewählte Form eine bessere Handhabung des Transparenzgebots, da die betroffene Person sich hierdurch besser informieren kann. Dieser Zielkonflikt muss aufgelöst werden, wobei insbesondere auf weitere Gestaltungsmöglichkeiten und Erweiterungen einzugehen ist.

7.3 ISÆN-Blockchain

ISÆN hat das Ziel, die Schutzprinzipien „Transparenz“ und „Nachvollziehbarkeit“ bezüglich der Weitergabe personenbezogener Daten technisch zu stärken. Dazu wird eine Blockchain genutzt, um Informationen über die Weitergabe personenbezogener Daten zu speichern. In diesem Abschnitt werden offene Punkte aufgezeigt, die sich durch die Nutzung einer Blockchain in ISÆN ergeben.

7.3.1 Erfüllung der Sicherheitsvoraussetzung der Blockchain

Der Einsatz einer Blockchain setzt voraus, dass keine Partei zu einem Zeitpunkt mehr als 50 Prozent der Rechenleistung aller der am Blockchain-Netzwerk teilnehmenden Parteien besitzt. Vor dem Einsatz einer Blockchain in einer Anwendung muss die Erfüllung dieser Voraussetzung sichergestellt werden. Im Falle von ISÆN kommen die Mobiltelefone der betroffenen Personen aufgrund ihrer beschränkten Ressourcen (Rechenleistung, Akku, Speicherplatz, keine permanente Internetverbindung) voraussichtlich nicht als Teilnehmer des ISÆN-Blockchain-Netzwerks in Frage.

Die Annahme, dass niemand über mehr als 50 Prozent der Ressourcen verfügt, könnte in der Praxis äußerst schwer sicherzustellen sein. Insbesondere lässt sich aus der Erfüllung dieser Annahme bei Inbetriebnahme der Blockchain nicht schließen, dass sie auch zu einem späteren Zeitpunkt erfüllt sein wird. Beispielsweise kann sich über die Zeit oder durch die Änderungen von Anreizen für die Partizipation die Anzahl der Teilnehmer des Netzwerks reduzieren, was es einfacher macht, die Kontrolle über einen kritischen Teil der Ressourcen zu erlangen. Im schlimmsten Fall könnten Teilnehmer sogar zusammenarbeiten, um Änderungen am Inhalt der Blockchain zu forcieren (wie jüngst erst bei Ethereum geschehen – vgl. Abschnitt 6.2.6.1.2). Die Annahme über die Verteilung der Ressourcen im Blockchain-Netzwerk unterscheidet sich daher grundsätzlich von Annahmen über die Sicherheit von klassischen kryptographischen Verfahren, da deren Entwicklung in der Regel für die nähere Zukunft abgeschätzt werden kann.

7.3.2 Transparenz und Unveränderlichkeit

Eine wesentliche Eigenschaft der Blockchain ist, dass der gespeicherte Inhalt transparent für alle Blockchain-Nutzer sichtbar ist. Darüber hinaus, können in der Blockchain gespeicherte Daten nicht verändert oder gelöscht werden (vgl. Abschnitt 6.2). Aus diesem Grund bieten sich Blockchains als sicherer dezentraler Speicher für Transaktionen an.

Aus der Unveränderlichkeit einmal gespeicherter Inhalte folgt, dass nach der DSGVO in einer Blockchain keine personenbezogenen Daten gespeichert werden dürfen. Hieraus entsteht ein Zielkonflikt: Einerseits müssen Einwilligungen für betroffene Personen und Verantwortliche nachvollziehbar gespeichert werden, andererseits müssen diese Daten gegenüber Dritten geschützt werden. Potenzielle hieraus entstehende Zielkonflikte sind im angedachten deutsch-französischen Projekt unter Betrachtung konkreter Anwendungsfälle frühzeitig aufzulösen.

Die Einführung einer Public-Key-Infrastruktur und beispielsweise eintragsspezifischer Schlüsselpaare, bei denen die Verantwortlichen und die betroffenen Personen den geheimen Schlüssel oder eintragsspezifische Identifier kennen, könnten potenziell diesen Zielkonflikt für die vorgeschlagene Architektur in ISÆN auflösen. Dadurch ergeben sich jedoch wiederum Herausforderungen für das Schlüssel- oder Identitätsmanagement und als Resultat eine verminderte Nutzbarkeit für betroffene Personen. Eine konkrete Umsetzung von ISÆN muss alle Anforderungen, wie beispielsweise die Nachweisbarkeit von Einwilligungen, erfüllen.

7.3.3 Dezentralität und Kosten

Ein großer Vorteil der Blockchain-Technologie ist die

dezentrale unveränderliche Speicherung. Diese Dezentralität und Autonomie erzeugen aber vergleichsweise hohe Kosten im Vergleich zu einer zentralen vertrauenswürdigen Stelle, welche die Daten und Transaktionen ebenso speichern könnte, bzw. zu einem alternativen System, das ohne dritte Stelle auskommt (vgl. Abschnitt 7.3.6). Die Erstellung neuer Blöcke in einer Blockchain kostet eine enorme Menge an Energie (Proof-of-Work-Konzept). Es entstehen Kosten für Bandbreite und CPU-Zeit aller Teilnehmer des Blockchain-Netzwerks, die in irgendeiner Weise kompensiert werden müssen. Dies geschieht im Allgemeinen durch eine Entlohnung für das Erstellen neuer Blöcke und durch zu zahlende Transaktionsgebühren. Die Gesamtkosten hängen von der Größe der in der Blockchain zu speichernden Informationen ab, und insbesondere davon, wie häufig Daten (Transaktionen) geschrieben werden.

Eine Alternative zum Proof-of-Work-Konzept stellt das umstrittene Proof-of-Stake-Konzept dar, das bei der Erstellung eines neuen Blocks mit weniger Energie auskommt, aber zahlreiche andere Schwierigkeiten beim Herstellen eines Konsenses zwischen allen verteilten Knoten mit sich bringt.

Ziel des ISÆN-Konzepts ist es, Dezentralität und Autonomie von Verträgen zwischen betroffenen Personen und verantwortlichen Stellen zu erreichen. Konkrete Ausgestaltungen müssen eine Balance zwischen diesen Anforderungen und den daraus resultierenden Kosten sowie der gesteigerten Komplexität des Gesamtsystems finden.

7.3.4 Skalierung

Neben den Fragen bezüglich der durch den Betrieb der Blockchain entstehenden Kosten ergibt sich auch die Frage der Skalierung, d. h. die Frage, ob das dezentrale Netzwerk ausreichend Transaktionen pro Sekunde bewerkstelligen kann, bei gleichzeitig ausreichend hohem Vertrauen und ausreichend hoher Sicherheit. Aufgrund der Funktionsweise einer Blockchain ist das Datenspeichervermögen stark begrenzt. Ausschlaggebend ist die maximale Größe eines Blocks in der Blockchain. Die Größe eines Blocks muss begrenzt werden, um die Propagation im Blockchain-Netzwerk konstant zu halten und um den Rechenaufwand bei der Erzeugung eines neuen Blocks zu begrenzen.

Diese Thematik ist aktuell und bereits seit einiger Zeit Forschungs- und Diskussionsgegenstand. An dieser Stelle sei auf die Diskussion im Bitcoin-Netzwerk verwiesen.[47]

7.3.5 Neue Blockchain vs. Operation auf vorhandener Blockchain

Prinzipiell ist es möglich, für eine Anwendung eine neue Blockchain aufzubauen oder eine bestehende Blockchain zu verwenden.

Neben der eigentlichen, dezentralen Blockchain bedarf es zum Betrieb einer Blockchain einer großen Anzahl von Netzwerkknoten sowie erfahrungsgemäß einer Menge weiterer Services, die betrieben und bereitgestellt werden müssen.[48] Diese Services, wie z. B. Online-Analyse-Tools und Tauschbörsen, sind für eine gute Benutzbarkeit unabdingbar. Setzt man auf eine bestehende Blockchain auf, ist diese Infrastruktur meist schon vorhanden. Im Hinblick darauf bietet es sich an, mit einer vorhandenen Blockchain zu arbeiten. Nachteil dieser Variante ist die höhere Komplexität dieser Lösung. Eine weitere Möglichkeit ist der Betrieb einer so genannten Side Chain[49] oder auch der Off-Chain-Handel von Abmachungen und Verträgen unabhängig von der Blockchain, jedoch mit der Sicherheit, dass zu jedem Zeitpunkt der signierte Vertrag durch Einbringen in die Blockchain geltend gemacht werden kann. Beide Möglichkeiten entlasten die Haupt-Blockchain und sparen dadurch Energie und Geld. Allerdings steigt die Komplexität des Gesamtsystems jeweils enorm an.

7.3.6 Alternative technische Ausgestaltungsmöglichkeiten und Erweiterungen des ISÆN-Konzepts

Alternativ zur vorgeschlagenen Architektur ist auch denkbar, dass Einwilligungen lokal von beiden Seiten (betroffene Person und Verantwortliche) signiert jeweils in der Ævatar-App und bei der verantwortlichen Stelle protokolliert werden. Zusätzlich könnte die Ævatar-App die Protokollierungen mit einem geheimen Schlüssel der betroffenen Person verschlüsselt in einem Cloud-Speicher ablegen, wodurch die betroffene Person die Ævatar-App auch auf mehreren Endgeräten benutzen kann. Diese Lösung erfüllt die Anforderungen bezüglich Transparenz und Nachvollziehbarkeit für betroffene Personen sowie Verantwortliche und verzichtet komplett auf eine Blockchain mit den oben genannten Herausforderungen.

7.4 ISÆN und Datennutzungskontrolle

Nachfolgend wird von der Annahme ausgegangen, dass das ISÆN-Konzept als lauffähiges System realisiert ist und seine Funktionalität über geeignete Schnittstellen interessierten Marktteilnehmern zur Verfügung gestellt werden kann. Das Sicherheitsframework „IND²UCE “ ist in diesem Szenario letztlich nichts anderes als ein weiterer Marktteilnehmer, der die Eigenschaften und Effekte des Gesamtkonzepts zur Optimierung der eigenen Fähigkeiten einsetzt.

Für die Eignungsanalyse im Hinblick auf die Unterstützungsmöglichkeiten zur Datennutzungskontrolle wird von folgenden Eigenschaften ausgegangen:

Die ISÆN ist ein strukturiertes Datum, mit dessen Hilfe sich natürliche Personen unmittelbar, d. h. ohne zusätzliche Hilfsmittel, eindeutig identifizieren lassen. Die konkrete ID

- setzt sich aus mehreren personenbezogenen Merkmalen zusammen,
- identifiziert bereits in der kanonischen Form eindeutig,
- bleibt über den gesamten Verwendungszeitraum unverändert,
- besitzt einen irreversiblen (ebenfalls eindeutigen) Hashwert,
- sollte in öffentlichen Netzen nur als irreversibler Hashwert vorliegen.

ISÆN stellt einen Dienst zur Lokalisierung personenbezogener Daten bzw. Verfolgung von Datentransfers im Internet zur Verfügung. Die konkrete Dienstleistung

- wird durch das Zusammenwirken unabhängiger vertrauenswürdiger Dienstleister (durch ein nicht näher spezifiziertes Protokoll) realisiert,
- kann jederzeit und überall von jedem Stakeholder genutzt werden,
- besteht darin, die Aufenthaltsorte und Transferwege personenbezogener Daten (in einem Blockchain-Netzwerk) revisionssicher zu dokumentieren,
- besitzt mindestens zwei (nicht näher spezifizierte) Schnittstellenfunktionen: eine Protokollfunktion, um den Sachverhalt eines Datentransfers zu hinterlegen, und eine Recherchefunktion, um entsprechende Sachverhalte in Erfahrung zu bringen.

Wie lassen sich nun diese Eigenschaften im Rahmen des Sicherheitsframeworks „IND²UCE “ nutzen? Grundsätzlich sind hier zwei Verwendungsmöglichkeiten denkbar: Zum einen könnten bislang unbekannte Nutzungskontexte im Zusammenhang mit der Verarbeitung personenbezogener Daten anhand des Zugriffs auf ISÆN-spezifische Datenstrukturen oder Funktionen erkannt werden. Zum anderen könnte die von ISÆN bereitgestellte Funktionalität genutzt werden, um – für den Nutzer bestenfalls transparent – Informationen über die Verwendung und den Transfer personenbezogener Daten dort zu hinterlegen bzw. zu recherchieren. Beide Möglichkeiten werden im Folgenden diskutiert.

7.4.1 ISÆN zur Kontexterkennung

Die Grundmotivation für das ISÆN-Konzept liegt darin, ein Rahmenwerk zu schaffen, über das sich vorgege-

bene Datenschutzziele auf nationaler und internationaler Ebene einfach und pragmatisch umsetzen lassen. ISÆN soll dabei – ungeachtet einer gegebenenfalls verteilten Umsetzung – eine zentrale Anlaufstelle schaffen, die immer dann zwingend einzubinden ist, wenn das Recht auf die Verarbeitung personenbezogener Daten von einem hierzu berechtigten Dienstleister A auf einen bislang unberechtigten Dienstleister B übergegangen ist. Dieser Sachverhalt manifestiert sich letztlich im Aufruf der Protokollfunktion von ISÆN, wodurch die bezeichnenden Merkmale dieser Rechtetransaktion transparent und revisionssicher hinterlegt werden.

Der Aufruf der Protokollfunktion ist somit im Kontext der Verarbeitung personenbezogener Daten ein bedeutsames Ereignis, dessen Auftreten durch das Sicherheitsframework „ IND²UCE “ über einen PEP (Policy Enforcement Point) erkannt und anschließend im Rahmen des Event-Condition-Action-Paradigmas über den PDP (Policy Decision Point) und PXP (Policy Execution Point) behandelt werden kann. Der konkrete Nutzen ist inhärent situationsspezifisch und soll daher durch ein kleines einfaches Beispiel veranschaulicht werden: Es wird angenommen, dass das Recht zur Verarbeitung der Daten – sei es aufgrund schlechter Erfahrungen oder infolge restriktiver Unternehmenspolitik – nur für eine begrenzte Zeit gewährt werden soll. IND²UCE könnte nun einfach durch eine entsprechende Richtlinie automatisch und transparent dafür sorgen, dass der gewährende Besitzer der Daten zu einem gegebenen Zeitpunkt (oder bei Bedarf auch wiederkehrend) daran erinnert wird, seine Datenfreigaben wieder zurückzunehmen.

Die Dokumentation des Datentransfers durch Aufruf der Protokollfunktion ist nur ein abschließender Schritt, dem im Vorfeld zunächst die Absicht zum Datentransfer und daran anschließend die spezifische Zustimmung durch den Dateneigentümer vorausgegangen sein müssen. Diese Schritte sind dabei unabhängig und losgelöst von Schnittstellenfunktionen bzw. konkreter Realisierung von ISÆN. Das Konzept geht lediglich davon aus, dass ein (nicht näher spezifizierter) Benachrichtigungsmechanismus existiert, über den sich Dateneigentümer und die beteiligten Dienstleister bezüglich Absicht und Zustimmung gegenseitig informieren können.

Die Nutzung des Benachrichtigungsmechanismus, also das Senden und Empfangen entsprechender Nachrichten, liefert damit weitere bedeutsame Ereignisse, die einen spezifischen Kontext im Zusammenhang mit der Verarbeitung personenbezogener Daten definieren. Wie schon bei der Protokollfunktion lassen sich diese Kontexte anhand der auslösenden Ereignisse durch IND²UCE einfach erkennen und situationsabhängig behandeln. So ist z. B. eine Richtlinie denkbar, welche die Anfragen „lästiger“ Dienstleister ohne weitere Rücksprache mit dem Dateneigentümer blockt bzw. mit einem negativen Bescheid quittiert. Die Kriterien, nach denen ein bestimmter Dienstleister als „lästig“ einzustufen ist, ließen sich dabei flexibel in der Richtlinienspezifikation, beispielsweise anhand des Überschreitens einer bestimmten Anfragehäufigkeit oder auch explizit durch Angabe von Namen oder Adressen, festlegen.

Eine weitere Möglichkeit, besondere Nutzungskontexte der personenbezogenen Datenverarbeitung zu erkennen, eröffnet sich durch die Überwachung von Zugriffen auf Datenstrukturen, die den Datenwert der ISÆN in irgendeiner Form repräsentieren – was mit IND²UCE bei androidbasierten Systemen auf Basis von TaintDroid prinzipiell möglich wäre. Entsprechende Zugriffe könnten dann als Indiz dafür gesehen werden, dass im Sinne des ISÆN-Konzepts interagiert wird bzw. interagiert werden soll. Auffälligkeiten wie z. B. das Abweichen von üblichen Zugriffsmustern ließen sich so gegebenenfalls anhand von Richtlinien spezifizieren und durch geeignete Maßnahmen, wie z. B. die Benachrichtigung der betroffenen Nutzer oder das Sper-

ren weiterer Zugriffe, begegnen. Denkbar ist darüber hinaus die Verknüpfung mit anderen Ereignissen bzw. Ereignistypen, die eine Eingrenzung des Nutzungskontextes und damit letztlich auch die Möglichkeit einer spezifischen angemessenen Behandlung zulassen. So könnte z. B. das Mailen einer unverschlüsselten ISÆN oder deren Speicherung auf einem USB-Stick durch das System entweder kategorisch verhindert oder gegebenenfalls erst nach einem expliziten Bestätigungsschritt gewährt werden.

7.4.2 ISÆN zur Kontextbehandlung

Das ISÆN-Konzept geht von der Grundüberlegung aus, dass die heute am Markt befindlichen Dienstleister und Organisationen bereits über eine Vielzahl von Systemen verfügen, in denen personenbezogene Informationen in großen Daten-Repositorys (Enterprise Data Lakes) in irgendeiner Form bereits gespeichert sind. Zusätzlich wird davon ausgegangen, dass es einen Mechanismus (Opt-in-/Opt-out-Management) gibt, über den der Dateneigentümer bestimmen kann, wer in welcher Weise auf seine Daten zugreifen darf. Dabei spielt es aufgrund der gewählten Abstraktion keine Rolle, wie die Systeme, Mechanismen oder funktionalen Schnittstellen konkret realisiert und beschaffen sind. Wesentlich aus Konzept-Sicht ist nur, dass die vorausgesetzte prinzipielle Grundfunktionalität zuverlässig und angemessen erbracht wird.

Im Zusammenhang mit der Frage, ob und wie sich das Konzept zur Behandlung von Nutzungskontexten einsetzen lässt, sind dabei speziell die beiden (nicht näher spezifizierten) Schnittstellen zum Protokollieren und zum Recherchieren gewährter Datentransfers von Interesse.

In der Terminologie von IND²UCE dient ISÆN technisch gesehen als PIP (Policy Information Point), der bei Bedarf zum Abruf oder zur Speicherung situationsspezifischer Informationen herangezogen wird. IND²UCE kann diesen PIP dann im Rahmen der Ereignisbehandlung durch den PDP (Policy Decision Point) nutzen, um im Hintergrund – also transparent für den Anwender – Aktionen durch den PXP (Policy Execution Point) anzustoßen, die als Seiteneffekt insbesondere auch Abläufe enthalten, bei denen der Transfer personenbezogener Daten (oder das Wissen um entsprechende Transfers) inbegriffen ist.

Beispielsweise könnte auf diese Weise sehr einfach und bequem die bereits im ISÆN-Konzept angedachte Funktion eines persönlichen Datenschutz-Ævatars mit den Mitteln von IND²UCE realisiert werden. Bei einem solchen Ævatar handelt es sich um einen persönlichen virtuellen Agenten, der stellvertretend für den Dateneigentümer Entscheidungen im Hinblick auf die Verwendung, Speicherung und Weitergabe personenbezogener Daten treffen soll und durchsetzen kann. Das Verhalten eines Ævatars ließe sich dabei mit einfachen typischen IND²UCE -Mitteln durch Formulierung individueller Richtlinien kontextspezifisch nachbilden. Absage oder Gewähr solcher Anfragen könnten so automatisiert, also ohne weitere Interaktion mit der betroffenen Person im Hintergrund erledigt werden.

Denkbar sind aber auch komplexere Anwendungen, wie die Realisierung eines innerbetrieblichen Auskunftssystems, das situationsabhängig mit personenbezogenen Informationen befüllt wird. So könnten z. B. Namenslisten, die in der einfachsten Form nur Vor- und Nachnamen enthalten, im Lauf der Zeit mit spezifischeren Einzelmerkmalen angereichert werden. Die personenbezogenen Merkmale und insbesondere deren Nutzungsfreigabe ließen sich dabei – ausgelöst durch entsprechende Richtlinien im Rahmen des IND²UCE -typischen Event-Condition-Action-Paradigmas – durch Hintergrundanfragen bei bekannten, vertrauenswürdigen Dienstleistern zusammentragen. Entsprechende Einwilligungen vorausgesetzt, ließe sich durch Einsichtnahme und Rückverfolgung der Datenspuren im ISÆN womöglich sogar eine Historie der Anstellungen eines Arbeitnehmers in Erfahrung bringen.

Im Grunde sind noch viele weitere Anwendungsfälle denkbar, die sich aus der Nutzung von ISÆN als PIP ergeben könnten. Grenzen setzen hier zum einen nur die (bekannten) rechtlichen Vorgaben, die z. B. aus der erst kürzlich verabschiedeten DSGVO folgen. Die sich daraus ergebenden Einschränkungen sind im Wesentlichen bekannt oder berechenbar bzw. können bei Bedarf recherchiert und von entsprechend geschulten Fachleuten diskutiert werden. Grenzen setzt zum anderen aber auch der (unbekannte) technische und organisatorische Rahmen, innerhalb dessen ein System wie ISÆN operieren soll. Da bislang nur eine vage Vision hinsichtlich der zu realisierenden Funktionalität und wenig Konkretes über die Ausgestaltung von Aufgaben, Schnittstellen und Funktionen eines solchen Systems bekannt sind, öffnet sich hier ein nahezu grenzenloser Raum für Spekulation und Möglichkeiten. Letztlich resultiert daraus zumindest im Moment noch eine unüberschaubare Vielfalt, die eine umfassende und abschließende Behandlung und Beurteilung des Konzepts aktuell nicht möglich macht und in einem nächsten Schritt durch entsprechende Konkretisierungen und Verfeinerungen der ISÆN-Konzeption deutlich reduziert werden sollte.

7.5 Potenzial des ISÆN-Konzepts

Da der Anwender sich jederzeit darüber informieren können soll, welche Dienstanbieter seine personenbezogenen Daten erhalten haben, könnte ISÆN dazu beitragen, das Gebot der Transparenz zu stärken. Beispielsweise kann ISÆN dem Anwender ermöglichen, gezielter Verantwortliche zu identifizieren, gegen die er anschließend seine Betroffenenrechte geltend machen kann. Er kann dann entsprechend von seinem Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrecht Gebrauch machen. Wenn sich in einer konkreten technischen Ausgestaltung jedoch durch eine Verknüpfung ein Personenbezug der in der Blockchain gespeicherten Daten ergibt, hat die betroffene Person das Recht, die Löschung zu veranlassen. Aufgrund der technischen Konzeption ist eine Löschung in der Blockchain allerdings nicht möglich. Dies muss in Bezug auf eine Erweiterung des ISÆN-Konzepts berücksichtigt werden. Dadurch, dass vorgesehen ist, dass der Nutzer schrittweise die Verwendung seiner Daten bestätigt, kann dieser eine bewusste Entscheidung über die Weitergabe treffen. Darüber hinaus kann der Nutzer gezielt festlegen, welche Daten er an Dienstleister weitergeben möchte. Einer inflationären Weitergabe von Daten, die für die Abwicklung des konkreten Geschäfts nicht notwendig sind, könnte damit entgegengewirkt werden. Dadurch und durch die Bestätigung der Datenweitergabe bei jeder Anfrage wird zugleich der Zweckbindungsgrundsatz berücksichtigt. Durch die Einbindung von biometriebasierten Authentifikationsverfahren können die personenbezogenen Daten des Nutzers benutzerfreundlich geschützt werden.

In den Fällen, in denen eine gesetzliche Legitimation (wie im hier beschriebenen Anwendungsfall) nicht gegeben ist, könnte die ISÆN auch bei der Einholung einer Einwilligung unterstützend wirken, da sie durch die Anfrage an den Anwender diesem die Möglichkeit eröffnet, eine entsprechende Einwilligung zu erteilen. Zu bedenken ist jedoch auch hier, dass eine solche Einwilligung jederzeit widerrufbar sein muss. Wenn sich nachträglich ein Personenbezug generieren lässt, ist eine technische Ausgestaltung mittels Blockchain nicht geeignet einen etwaigen Widerruf adäquat umzusetzen.

Weiterhin unterstützt ISÆN den Verantwortlichen zumindest partiell bei der Erfüllung seiner Informationspflichten. Dieses Potenzial sollte weiterhin ausgeschöpft werden. Hierbei sollte jedoch sichergestellt werden, dass eine nachträgliche Verknüpfung mit den Realdaten ausgeschlossen ist. Das Speichern in der Blockchain stellt auch für den Dienstanbieter eine Möglichkeit dar, gezielt Vorgänge protokollieren zu lassen. Gleichwohl besteht auch hier die Notwendigkeit, eine Zuordnungsmöglichkeit auszuschließen.

7.6 Zusammenfassung der Bewertung

Die Idee, den Schutz personenbezogener Daten durch technische Maßnahmen zu stärken, sollte in unserer heutigen digitalisierten Gesellschaft zwingend weiterverfolgt werden. In konkreten Anwendungen, welche die hinter dem ISÆN-Konzept stehenden Ideen umsetzen, müssen allerdings zusätzliche rechtliche und technische Fragen geklärt werden. Grundsätzlich sollte die Verwendung von Identifizierungssystemen auch im Privatsektor gestärkt werden, um das Vertrauen in den elektronischen Geschäftsverkehr entsprechend zu stärken. Gleichzeitig wird durch die Speicherung verschiedener Aspekte, wie der Änderung von eingegebenen Daten, der Anfrage von Dienstanbietern und der entsprechenden Autorisierung der Speicherung und Verarbeitung der Daten, die Nachvollziehbarkeit erhöht. Aus datenschutzrechtlicher Sicht muss angedacht werden, das Konzept dahingehend zu erweitern, dass eine Möglichkeit der Zuordnung von öffentlich gespeicherten Daten zu den Realdaten ausgeschlossen ist. Beispielsweise sollte die Nutzung eines entsprechenden neuen Pseudonyms für jede einzelne Transaktion in Erwägung gezogen werden, um das Risiko einer Identifizierung so gering wie möglich zu halten. Die Verwendung eines einsehbaren Speichers kann sowohl für den Dienstanbieter im Hinblick auf entsprechende Dokumentations- und Informationspflichten als auch für die betroffene Person hilfreich sein, um sich in transparenter Weise zu erkundigen, wem entsprechende Zugriffe auf Daten erteilt wurden. Dadurch könnte sich die betroffene Person gezielter an entsprechende Verantwortliche wenden, um ihre Betroffenenrechte geltend zu machen.

Die Vorteile der Dezentralität und die grundsätzlich hierdurch ermöglichte Nachvollziehbarkeit können durch ISÆN voll ausgeschöpft werden. Insofern sollte das Konzept von ISÆN nach dem Appell der DSGVO weiter ausgebaut werden, um sicherzustellen, dass ein Rückschluss auf die Identität etwaiger Anwender nicht möglich ist.

8 Anwendungsfall „E-Health Infrastruktur in Deutschland“

Wie in Abschnitt 5.1 beschrieben, wurde in Deutschland zum 01.01.2015 eine elektronische Gesundheitskarte mit der eGK-Nummer als Identifier des Patienten eingeführt. Trotz der dafür getätigten erheblichen Investitionen der Krankenkassen und der seit mehr als 10 Jahren angestrebten Telematik-Infrastruktur für das deutsche Gesundheitswesen bleibt der konkrete Nutzen der E-Health-Infrastruktur für den einzelnen Patienten und die Gesellschaft bisher weit unter den Erwartungen.

Mit dem am 29.12.2015 in Kraft getretenen E-Health-Gesetz wurden vom Gesetzgeber nun Fristen und Verantwortlichkeiten für die Einführung konkreter Anwendungen auf Basis der eGK-Technologie vorgegeben. Diese können im Vergleich zu europäischen Standards in Skandinavien aber auch zum Baltikum und zu Großbritannien jedoch nur als ein erster Schritt hin zu einer vernetzten Versorgung angesehen werden. Mit den im E-Health-Gesetz vorgeschriebenen sechs eGK-Anwendungen

1. Versichertenstammdatenmanagement – ab Mitte 2016 Versichertenstammdaten auf der eGK,
2. elektronischer Arztbrief – ab 2017 unstrukturierte Informationsübermittlung zwischen Medizinern auf der eGK als Datenträger, z. B. bei Krankenhausentlassungen,
3. Medikationsplan in Papierform mit Barcode ab 01.10.2016 – in strukturierter (extra vergüteter) elektronischer Form auf der eGK ab 01.01.2018 – verpflichtend nur bei mehr als drei gleichzeitig verordneten Medikamenten,
4. Notfalldatenmanagement – ab 2018 (extra vergütete) Speicherung strukturierter notfallrelevanter medizinischer Informationen zu Allergien, Vorerkrankungen oder zu Implantaten durch ambulante Ärzte auf der eGK,
5. „Patientenakte“ – ab 2019 Übertragung von Befunden, Arztbriefen, Medikationsplan sowie medizinischen Dokumenten wie Impfpass oder Mutterpass auf die eGK,
6. Patientenfach – ab 2019 soll es Patienten möglich sein, selbst Daten in einem Onlinefach zu speichern und diese auch außerhalb der Arztpraxis einzusehen, beispielsweise selbst gemessene Blutzucker- oder Blutdruckwerte

lassen sich allenfalls grobe Informationsdefizite bei ärztlichen Entscheidungen (mit teilweise tödlichen Folgen) verringern, und dies auch nur dann, wenn es gelingt, den jahrzehntelangen Abwehrreflex praktizierender Mediziner zu überwinden.

Dies wird nur gelingen, wenn Patienten selbst einen persönlichen Nutzen wahrnehmen und im Eigeninteresse die Informationsübermittlung einfordern und ermöglichen. Die am 10.10.2016 auf dem World Health Summit in Berlin vorgestellte Vermächtnisstudie des WZB für Sozialforschung zeigt, dass das Thema Gesundheit für die Deutschen auf der Werteskala weit nach oben gewandert ist.

Das ist jedoch weniger ein Verdienst des Gesundheitswesens, sondern vielmehr eine positive Auswirkung der digitalisierten Informationsgesellschaft, in der das Wissen über innovative Diagnose- und Behandlungsmöglichkeiten, aber auch das Monitoring der eigenen Vitalwerte und der Wirkung von Bewegungs- und Ernährungsgewohnheiten längst nicht mehr den ausgebildeten Medizinern vorbehalten sind. Als Folge einer sich rasant entwickelnden Mobile-Health-Industrie verfügen auch ältere Patienten heute sowohl über zahlreiche selbst recherchierte Informationen als auch über selbst (z. B. per Wearables, Messgeräte oder Smartphones) erfasste Gesundheitsdaten. In diesem neuen Sektor der Gesundheitswirtschaft – als größte Branche Deutschlands – entstehen dabei höchst wertvolle Datenschätze die auch nach Umsetzung des aktuellen E-Health-Gesetzes für den behandelnden Mediziner nicht zur Verfügung stehen.

Dabei entwickelt sich insofern ein Paradoxon, als Patienten die (oft aus nicht validierten Quellen) erworbe-

nen Informationen und Ihre selbst (meist auf kommerziellen Infrastrukturen) erfassten Gesundheitsdaten als sicher, teilbar und transparent empfinden, während die in der Regelversorgung entstehenden, weitaus besser gesicherten Routinedaten zur Diagnostik und Therapie als Black Box und unverständlich/nicht nutzbar eingeschätzt werden. Der (selbst)informierte Patient sieht sich zunehmend als gleichberechtigter Akteur und Entscheider in Gesundheitsfragen und verfügt bereits heute zunehmend über andere sowie nicht selten über mehr Informationen als sein behandelnder Arzt.

Um diese realen Probleme im deutschen Gesundheitswesen zu überwinden und die Chancen der Digitalisierung zu nutzen, wäre nichts weiter nötig als die Möglichkeit für den Patienten, seine von ihm selbst erfassten und seine in der Regelversorgung verteilt bei Leistungserbringern, Kassen und Dienstleistern gespeicherten Gesundheitsdaten im Überblick einzusehen, zu verfolgen und bewusst mit seinen medizinischen, aber auch therapeutischen und pflegerischen Behandlern (Behandlungsteams) teilen zu können. Die deutsche Telematik-Infrastruktur ist in der derzeit vorgesehenen Form dazu nicht geeignet. Einer der wesentlichsten Gründe dafür liegt in der Speicherchip-Technologie, die auf einer physischen Datenübertragung unter Nutzung des ausschließlich in der GKV verwendeten eGK-Identifiers beruht und damit den regelhaften Informationsaustausch mit nichtmedizinischen und nichtpflegerischen Professionen, aber auch mit kommerziellen mHealth-Anwendungen praktisch unmöglich macht. Daran ändert auch das für 2019 vorgesehene Online-Patientenfach nichts.

Erst durch eine niederschwellige Technologie, die dem Patienten selbst die Hoheit über seine verteilt gespeicherten Gesundheitsdaten gibt, wird es möglich sein, auch traditionelle Ärzte (laut OECD sind 42 Prozent der in Deutschland praktizierenden Ärzte 55 Jahre alt und älter) zur Nutzung einer E-Health-Infrastruktur zu bewegen und deren vielfach beschriebene Benefits für die Gesundheit des Einzelnen, das Gesundheitswesen und die gesamte Volkswirtschaft zu realisieren.

Hier eröffnet sich eine Anwendungsmöglichkeit für das ISÆN-Verfahren.

Vorstellbar ist, dass in einer Ausbaustufe der deutschen E-Health-Infrastruktur der Patient mittels eines von der Ævatar-App auf seinem Mobilgerät erzeugten QR-Codes die Zugangsdaten (nicht die Gesundheitsdaten selbst)

- zu allen vom ihm selbst auf mHealth-Anwendungen oder Messgeräten erfassten Gesundheitsdaten,
- zu allen bei seiner Krankenkasse über ihn vorliegenden Abrechnungsdaten,
- zu allen bei vom ihm beauftragten Dienstleistern (z. B. Pflegedienste und Therapeuten) erfassten Daten,
- zu allen im AIS von regelmäßig aufgesuchten Haus- und Fachärzten erfassten Behandlungsdaten,
- zu allen von ihm bei ausgewählten stationär tätigen Ärzten (Krankenhaus) und Pflegern (Pflegeheim) erfassten Behandlungsdaten

speichern und mit seinen persönlichen Daten (z. B. Notfalldaten) verknüpfen kann. Diese Zugangsdaten könnten dem Patienten z. B. über Barcodes von Dienstleistern, auf Basis von Institutskennzeichen (IK) und/oder der lebenslangen Arztnummer (LANR) von Leistungserbringern und der eGK der Krankenkasse physisch und per Smartphone lesbar bereitgestellt werden.

Die Ævatar-App sollte zudem die Möglichkeit bieten, durch intuitive Bedienung die eingescannten Zugangsdaten einzelner Datenquellen zu Behandlungsteams zu verknüpfen. Im Falle einer Zuordnung zu einem Behandlungsteam sollte die Verknüpfung an die Blockchain übertragen und dort ein verschlüsselter Austausch zwischen den beiden verknüpften Da-

tenquellen ermöglicht werden. Dabei könnten auch viewbasierte Verknüpfungs- und kryptographische Verfahren (wie z. B. im Federation-Server von SAS) zur Anwendung kommen, sodass gänzlich auf eine Datenübertragung zwischen verknüpften Quellen verzichtet werden kann. Eine Option „Erweitert“ sollte dem Patienten dabei die Möglichkeit geben, die verfügbaren Informationen in beiden zu verknüpfenden Quellen selektiv auszuwählen. Schließlich sollte über die Option „Verknüpfung Löschen“ jederzeit die Möglichkeit bestehen, die Verknüpfung wieder aufzuheben und damit sofort den Datenaustausch zu unterbrechen. Im Sinne der DSGVO könnte auch eine Option „Daten löschen“ in der Ævatar-App vorgesehen werden, um über einen entsprechenden „Delete“-Befehl an die Datenquelle das Recht des Patienten auf Datenlöschung technisch zu realisieren.

Falls es gelingt, eine solche vom Patienten konfigurierbare Verknüpfungs-Infrastruktur zu schaffen, wäre der Patient damit in der Lage,

1. alle Behandler seines Vertrauens zur gemeinsamen Nutzung seiner Gesundheitsdaten zu ermächtigen,
2. die sektorübergreifende Zusammenarbeit medizinischer, pflegerischer und therapeutischer Professionen zu ermöglichen,
3. diesen selektiv auch Zugang zu nicht im Gesundheitswesen erzeugten mHealth-Daten zu gewähren,
4. selbst einen Überblick über seine verteilten Gesundheitsdaten zu gewinnen und gegebenenfalls Löschaufträge auszulösen,
5. seine bereits erfassten Gesundheitsdaten selektiv für Forschungszwecke und Studien freizugeben

und vieles andere mehr.

Auch das zuständige Bundesgesundheitsministerium hat die Limitationen der bisher angestrebten deutschen E-Health-Infrastruktur bereits erkannt und im Rahmen des Deutschen Kongresses für Versorgungsforschung am 05.10.2016 angekündigt, eine Studie zur Weiterentwicklung der deutschen E-Health-Infrastruktur in Auftrag zu geben. Im Rahmen dieser Studie könnte die Untersuchung der Einsatzmöglichkeiten des französischen ISÆN-Verfahrens für den Ausbau der deutschen E-Health-Infrastruktur detailliert erfolgen und gegebenenfalls zu einem gemeinsamen deutsch-französischen Standard für eine E-Health-Infrastruktur führen, die den Vorgaben der DSGVO entspricht und erheblichen Nutzen für Patienten und Gesellschaft durch selbstbestimmtes Information Sharing erzeugen kann.

Fußnoten

1 Dies gilt selbstverständlich ausschließlich dann, wenn die beteiligten Unternehmen ISÆN in ihrer Infrastruktur implementieren. Ein missbräuchliches Kopieren und Weiterverarbeiten der Daten kann auch mit ISÆN nicht verhindert werden.

2 https://wiki.oasis-open.org/xdi/FrontPage

3 Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO).

4 Spindler/Rockenbauch, Die elektronische Identifizierung. Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste, MMR 2013, 139

5 Spindler/Rockenbauch, Die elektronische Identifizierung. Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste, MMR 2013, 139, 141.

6 Eine Verpflichtung hierzu besteht nicht. Wenn jedoch eine unionsweite Verwendung angestrebt wird, muss eine Identifizierung erfolgen.

7 Siehe auch Jandt, Beweissicherheit im elektronischen Rechtsverkehr, NJW 2015, 1205, 1209; siehe auch ausführlich, ob ein indirekter Einfluss auf die Beweisvorschrift in § 371 a Abs. 1, 3 ZPO denkbar ist, Roßnagel, Beweiswirkungen elektronischer Vertrauensdienste, MMR 2016, 647, 648.

8 Roßnagel, Neue Regeln für sichere elektronische Transaktionen, NJW 2014, 3686, 3690.

9 Die Verordnung wird daher vielfach als „Richtlinie im Verordnungsgewand“ bezeichnet, so beispielsweise Kühling/Martini, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448, 448.

10 EuGH, NJW 2014, 2257 Rn. 52 ff. – Google Spain/AEPD.

11 Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios (2015), Datenschutzrecht, 3. Aufl., C.F. Müller, Heidelberg, Rn. 139.

12 Siehe auch Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841, 1845.

13 Wybitul, EU-Datenschutz-Grundverordnung in der Praxis, Was ändert sich durch das neue Datenschutzrecht? BB 2016, 1077, 1077.

14 Eickelpasch, Jörg (2016), „Die neue Datenschutzgrundverordnung“, Kommunikation und Recht, Beilage 1 zu Heft 9/2016, S. 22.

15 Vgl. insb. Volkszählungsurteil v. 19.12.1983 (BVerfGE 65, 1, S. 1).

16 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

17 https://en.wikipedia.org/wiki/Merkle_tree

18 https://en.bitcoin.it/wiki/Proof_of_work (siehe auch https://en.bitcoin.it/wiki/Proof_of_Stake und https://en.bitcoin.it/wiki/Proof_of_burn).

19 https://bitcoin.org/en/you-need-to-know

20 https://www.dgx.io/

21 https://www.ascribe.io/ und https://monegraph.com

[22] https://developer.ibm.com/dwblog/2016/blockchain-internet-of-things-iot/

[23] https://en.bitcoin.it/wiki/Weaknesses#Illegal_content_in_the_block_chain

[24] http://www.gruenderszene.de/allgemein/ethereum-dao

[25] https://de.wikipedia.org/wiki/OpenID

[26] https://joinup.ec.europa.eu/community/epractice/case/france-connect-id-federation-system-simplify-administrative-processes

[27] Schantz (2016) 1841, 1843.

[28] BfDI (2016), S. 10.

[29] Für weitere Fälle siehe Art. 6 DSGVO.

[30] Siehe hierzu Härting, Datenschutz-Grundverordnung, Rn. 89.

[31] Die im Nachfolgenden angegebenen Art. oder Erwägungsgrund sind ohne nähere Angaben solche der DSGVO.

[32] Kühling/Seidel/Sivridis (2015) Rn. 228.

[33] EuGH Breyer (Rs. C-582/14), Urteil vom 19.10.2016.

[34] Grundsätzlich zu bedenken ist, dass eine übergreifende Verwendung einheitlicher Personenkennzeichen durch private oder durch öffentliche Stellen in Deutschland als unzulässig erachtet wird, siehe Kirchberg, Personenkennzeichen – Ende der Privatsphäre?, ZRP 1977, Heft 6, 137. In seiner Mikrozensus-Entscheidung (BVerfGE 27, 1 ff.) hatte das Bundesverfassungsgericht zum Ausdruck gebracht, dass es mit der Menschenwürde nicht vereinbar ist, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme zugänglich ist“. Insoweit müsste untersucht werden, inwiefern beispielsweise notifizierte Identifizierungsmittel in derartiger Weise in Deutschland anerkannt werden können. Gleichwohl droht das Verbot einheitlicher Personenkennzeichen dadurch unwirksam zu werden, dass unterschiedliche Systeme auch ohne eine solche Nummer zusammengeführt werden können, siehe Kilian/Heussen-Weichert, 26, Ergänzungslieferung 2008, Teil 13, Rn. 38.

[35] Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 21.

[36] Roßnagel/Scholz, MMR 2000, 721, 724; siehe auch Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 21.

[37] Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 22.

[38] Creifelds (2014).

[39] Kühling/Seidel/Sivridis (2015), Rn. 214.

[40] EuGH, Urteil vom 09.11.2010, Verb. Rs. C-92/09 u. 93/09, Slg. 2010, I-11063-11161 – Veröffentlichung von Agrarbeihilfen, Rn. 53.

[41] Paal/Pauly-Ernst, Art. 4, Rn. 25.

[42] Der EuGH wendet in seinen datenschutzrechtlichen Entscheidungen die Art. 7 GRCh und Art. 8 GRCh nebeneinander an, siehe auch Paal/Pauly-Ernst,

Datenschutz-Grundverordnung, Art. 1, Rn. 6, mit entsprechenden Verweisen.

43 Siehe auch Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 65.

44 Siehe auch Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 39.

45 Siehe hierzu ausführlich Artikel-29-Datenschutzgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, WP 202.

46 Artikel-29-Datenschutzgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, WP 202, S. 21.

47 https://en.bitcoin.it/wiki/Scalability_FA

48 http://www.crypto20.org/blockchain-3-0-with-microsoft-bletchey-and-cryptlets

49 Back, Adam; Corallo, Matt; Dashjr, Luke; Friedenbach, Mark; Maxwell, Gregory; Miller, Andrew; Poelstra, Andrew; Timón, Jorge; Wuille, Pieter: Enabling Blockchain Innovations with Pegged Sidechains, https://blockstream.com/sidechains.pdf, 2014.

Abbildungsverzeichnis

Beteiligte Partner

FZI Forschungszentrum Informatik

PROF. DR.-ING. STEFAN JÄHNICHEN

... leitet die Begleitforschung des vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Technologieprogramms „Smart Data – Innovationen aus Daten“. Er ist Direktor am FZI Forschungszentrum Informatik und hat mehr als zwanzig Jahre das Thema Softwaretechnik an der Technischen Universität Berlin vertreten. Von 2008 bis 2011 war er Präsident der Gesellschaft für Informatik. 2013 erhielt er die Ehrendoktorwürde der Universität Potsdam.

PROF. DR. CHRISTOF WEINHARDT

... ist Leiter des Lehrstuhls für Information & Market Engineering am Karlsruher Institut für Technologie und Direktor am FZI Forschungszentrum Informatik. Seine Forschung konzentriert sich auf interdisziplinäre Themen aus dem Bereich Market Engineering mit Anwendungen in der IT-Dienstleistungsindustrie, der Energiewirtschaft sowie in Finanz- und Telekommunikationsmärkten. Am Karlsruher Institut für Technologie ist er Initiator und Leiter des Blockchain Networks, das Anwender unterschiedlicher Domänen aus Industrie sowie Forschung zusammenbringt und so die Konzeption und Weiterentwicklung von Blockchain-Lösungen vorantreibt.

PROF. DR. JÖRN MÜLLER-QUADE

... hat den Lehrstuhl für Kryptographie und Sicherheit am KIT inne, ist Direktor am FZI Forschungszentrum Informatik und Sprecher des Kompetenzzentrums für angewandte Sicherheitstechnologie. Er gewann mit Bingo Voting und Blurry Box zweimal den ersten Platz des Deutschen IT-Sicherheitspreises und ist acatech-Mitglied. Aktuelle Forschungsthemen mit bislang schwer erfüllbaren Datenschutzanforderungen sind beispielsweise Intelligente Infrastrukturen und die Energiewende, unbedenkliches Cloud Computing und eine datenschutzkonforme Überwachung öffentlicher Räume.

DR. MATTHIAS HUBER

... ist Abteilungsleiter im FZI Forschungszentrum Informatik. 2009 Abschluss des Studiums der Informatik am KIT mit anschließender Promotion. Von 2009 bis 2013 wissenschaftlicher Mitarbeiter am KIT. Seit 2013 als Abteilungsleiter im FZI. Forschungsschwerpunkte: Kryptographie und nachvollziehbare IT-Sicherheit, sichere Software-Architekturen, Datenschutz durch Technik, sicheres Datenbank-Outsourcing, Anonymitätsbegriffe und Datenbankanonymisierung.

DR.-ING. NICO RÖDDER

... promovierte im Bereich quantitativer Risikoanalyse und Failure Forecasting im IT-Service-Management am Karlsruher Institut für Technologie. Neben seiner Expertise in Methoden der Datenanalyse und –visualisierung, interessiert er sich beim Thema Blockchain insbesondere für Fragestellungen der systemimmanenten Architektur- und Anreizmechanismen dieser Technologie in unterschiedlichen Anwendungsszenarien. Am FZI Forschungszentrum Informatik leitet er die Abteilung Information Management & Analytics, in der zahlreiche Forschungs- und Industrieprojekte im Bereich Data Analytics, Service und Information Engineering bearbeitet werden.

DR.-ING. DAVID KARLIN

... leitet den Bereich Software Engineering am FZI. Er studierte Wirtschafsingenieurwesen an der Universität Karlsruhe (TH), heute Karlsruher Institut für Technologie (KIT), mit Schwerpunkten in Informatik und Business Process Engineering sowie Logistik und Supply Chain Management. Durch zahlreiche Tätigkeiten bei verschiedenen Unternehmen und Forschungsrichtungen in Deutschland und der Schweiz sowie einem Studienaufenthalt an der University of Technology in Sidney, Australien bringt er eine langjährige Erfahrung ein. Im Jahr 2015 schloss er seine Promotion als Doktor der Ingenieurwissenschaften am KIT ab.

ITSO GmbH

STEPHAN DROOFF

... ist seit 20 Jahren Geschäftsführender Gesellschafter der IT Service Omikron GmbH (ITSO), einem Softwaretechnik Spin-off der Fraunhofer-Gesellschaft. Schon in seiner Diplomarbeit hat er sich mit dem sicheren Austausch von Handelsdaten beschäftigt. Nach jahrelangem Frust mit kartenbasierten Identitätssystemen sieht er die Zukunft in Smartphone-basierten Konzepten wie der ISÆN. Handlungsdruck, um den europäischen und internationalen Rückstand Deutschlands bei der Nutzung von eIDs aufzuholen, erhofft er sich auch von der eIDAS-Verordnung.

UWE DER

... ist Diplom-Mathematiker und entwickelte bei Fraunhofer FIRST (heute FOKUS) Lösungen für Parallel- und Gridcomputing. Seit 2005 legt er als technischer Senior-Consultant bei der IT Service Omikron GmbH (ITSO) seine Schwerpunkte auf die Analyse und das Management von Projekten für öffentliche und private Aufraggeber sowie die Erstellung von technischen Gutachten und Spezifikationen. Aktuelle Trends der IT wie beispielsweise Blockchain untersucht er auf ihre Praxistauglichkeit - auch abseits der ausgetretenen Pfade.

Fraunhofer IESE

DR. JÖRG DÖRR

... ist seit 2010 Leiter der Hauptabteilung „Information Systems“ am Fraunhofer IESE in Kaiserslautern. Sein Arbeitsschwerpunkt in Forschungs- und Transferprojekten umfasst Requirements Engineering mit Fokus auf nicht-funktionalen Aspekten in dem er im Jahre 2010 auch promovierte. Jörg Dörr verfügt über umfassende Kenntnisse auf dem Gebiet des Requirements Engineerings für Software- und Systementwicklung und im Bereich Datennutzungskontrolle. Er leitet diverse Schulungs-, Technologietransfer- und Forschungsprojekte im industriellen Umfeld und ist Autor von mehr als 70 akademischen und industrienahen Publikationen. Seit 2006 ist er als Dozent zum Thema Requirements Engineering an Hochschulen aktiv.

SEBASTIAN HEUPTS

... ist wissenschaftlicher Mitarbeiter am Fraunhofer IESE in Kaiserslautern. Er arbeitet mit Industriekunden und in Forschungsprojekten an innovativen Architekturen und untersucht moderne Paradigmen und Technologien auf ihre Konsequenzen für die Gesamtqualität von Systemen. Sebastian Heupts ist in Projekten verschiedenster Domänen tätig, derzeit mit Schwerpunkt auf den Energiesektor.

DR. VOLKER HÜBSCH

... studierte Informatik und Mathematik an der Universität Kaiserslautern und promovierte auf dem Gebiet der verteilten Systeme. Seit 1997 arbeitet er als Senior Engineer am Fraunhofer-Institut für experimentelles Software Engineering IESE. In dieser Rolle war und ist er in Forschungs- und Industrieprojekten als Sicherheitsexperte und als Projektleiter tätig. Sein besonderes Interesse gilt der systematischen Entwicklung sicherer software-intensiver Systeme und skalierbaren Methoden zur Beurteilung und Garantie von IT-Sicherheit und Funktionssicherheit. Aktuelle Themen umfassen kontextabhängige Sicherheitsmechanismen sowie Konzepte zur flexiblen Steuerung der Datennutzung.

BBW-Hochschule

DR. THOMAS ZAHN

... ist seit 2013 Geschäftsführer des Gesundheitswissenschaftlichen Instituts Nordost (GeWINO) der AOK Nordost – Die Gesundheitskasse – und im April 2016 Professor für Wirtschaftsinformatik und Forschung an der bbw Hochschule in Berlin berufen. Vor seiner Tätigkeit beim Gesundheitswissenschaftlichen Institut Nordost war Professor Zahn Geschäftsführer des Elsevier Verlages, des HRI-HealthRisk Institute GmbH und der DxCG Gesundheitsanalytik GmbH. Er studierte medizinische Informatik, klinischen Management sowie Wirtschaftsinformatik in Deutschland und des USA. Thomas P. Zahn promovierte im Fachgebiet Neuroinformatik.

PETER SCHAAR

... ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz und war von 2003 bis 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Er wurde mit diversen Preisen ausgezeichnet, u. a. dem Preis der Friedrich-Ebert-Stiftung „Das politische Buch“, dem Sonderpreis der deutschen Internetwirtschaft des eco Forums 2008, als erster Preisträger mit dem GDD-Datenschutzpreis und dem Louis D. Brandeis Privacy Award.