IDENTITÄTSVERWALTUNG ÜBER DIE BLOCKCHAIN? RECHTLICHE BETRACHTUNGEN AM BEISPIEL DES INTERNETS DER DINGE

Anne Steinbrück

Anne Steinbrück, akademische Mitarbeiterin, Karlsruher Institut für Technologie (KIT), Forschungsgruppe Informationsrecht für technische Systeme und Rechtsinformatik (ITR)
Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe, DE
Anne.Steinbrueck@kit.edu; http://compliance.zar.kit.edu/21705.php

Schlagworte: ***Identitätsverwaltung, Blockchain, Internet der Dinge, eIDAS-VO, DSGVO***

Abstract: *Die Identitätsverwaltung umfasst die Verwaltung von kontextbezogenen Datensätzen im Internet der Dinge und verlangt die Kontrolle dieser Datensätze durch eine natürliche Person. Somit bedarf es der Identifizierung und der Verwaltung von Datensätzen etwa im Smart Home und am Smarten Arbeitsplatz. Diese kann dezentral über die Blockchain oder zentral über eine Trusted Third Party erfolgen. Jeweils ist ein gestuftes Vertrauens- und Sicherheitsmaß wünschenswert, mit dem die Anforderungen der eIDAS-VO und der DSGVO ihre Verwirklichung finden. Dabei könnte die Durchsetzung der Identitätsverwaltung über Smart Contracts erfolgen und über das ISAEN-Konzept realisiert werden.*

1. Einführung

Die Identitätsverwaltung ist die Steuerung von Datensätzen durch eine natürliche Person in einem spezifischen Kontext und kann das Internet der Dinge umfassen. Es kommt die Verwaltung in Kontexten etwa des *Smarten Arbeitsplatzes* oder des *Smart Home* und den darin verwendeten Komponenten in Betracht. Sobald im Internet der Dinge personenbezogene Daten zum Gegenstand der Verarbeitung werden, ist der rechtliche Schutzbereich des Rechts auf informationelle Selbstbestimmung nach dem deutschen Recht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und nach dem europäischen Schutz der Privatsphäre nach Art. 7, 8 EU-GrCharta richtungsweisend. Gleichzeitig sind zur Identitätsverwaltung Registrierungen erforderlich, die als Identifizierungsprozesse der eIDAS-VO und dem deutschen VDG unterliegen könnten. Diese Interdependenz von Recht und Technik im Internet der Dinge bedarf einer Kontrollmöglichkeit über ein Identitätsverwaltungssystem, bei dem die zentrale Steuerungsinstanz der Akteur «Mensch» bleiben muss. Insofern sollen im Folgenden der technische Rahmen für die Identitätsverwaltung in zentraler und dezentraler Hinsicht (2.), die rechtlich maßgeblichen Regelungskomplexe der DSGVO und der eIDAS-VO (3.) dargestellt werden und ein Ausblick (4.) erfolgen.

2. Technische Phänomene bei der Identitätsverwaltung

Die Identitätsverwaltung kann bezogen auf das Internet der Dinge über ein dezentrales System, der Blockchain (2.1.), oder ein zentrales System erfolgen (2.2.).

2.1. Dezentrales System

2.1.1. Die Blockchain als dezentrales System

Die Blockchain als dezentrales Transaktionssystem setzt an dem jeweiligen *Node*[1] als Eingabeinstanz an, bei dem eine natürliche Person eine Eingabe vornimmt. Dieser Eingabenwert wird in einem verteilt replizierten

[1] Vgl. Wattenhofer, The Science of the Blockchain (2016), S. 5, Definition: We call a single actor in the system node.

Datenblock (*Block*) gespeichert und dessen Verteilung erzeugt die allgemeine Transparenz. Ein Block wird durch einen Hashwert (vergleichbar mit einem «Fingerabrduck» der Blockinhalte) mit speziellen Eigenschaften vor Veränderungen und Manipulationen geschützt. Damit wird ein dezentraler Vertrauensanker als digitales Hauptbuch[2] begründet, welcher irreversibel ist.[3] Der neu errechnete Hashwert knüpft mit einem Zeitstempel an die Hashwerte der vorangegangenen Blöcke an, was eine allgemein transparente Kette von Blöcken zur Folge hat, sog. *chain*. Indem der Hashwert eines Blockes von den Hashwerten der vorangegangenen Blöcke abhängt, liegt darin ein weiterer Schutz vor potentiellen Manipulationen der Blöcke und der Blockinhalte. Dabei erfordert das *hashing* und *rehashing* für die Erweiterung der *chain* eine sehr hohe Rechenleistung.[4] Diesen Vorgang nennt man *Proof of work*[5].

Insgesamt kann die Blokchain in eine öffentliche und private Blockchain unterteilt werden. Die Differenzierung richtet sich danach, ob der Zugang zur Blockchain öffentlich ist oder einem beschränkten Nutzerkreis unterliegt.[6]

2.1.2. Der Smart Contract in der Blockchain

Der *Smart Contract*[7] in der Blockchain stellt die Umsetzung des vertraglich Vereinbarten über einen Algorithmus dar. Indem der *Smart Contract* als die Ausführung und Durchsetzung des vertraglich Vereinbarten dient, bedarf es für die Begründung des Outputs der Signaturen durch eine oder zwei Parteien.[8] Insofern ist die Bezeichnung aus rechtlicher Perspektive missverständlich, weil es sich nicht um einen Vertrag nach dem Bürgerlichen Gesetzbuch handelt, sondern um die Durchführung eines vorher verhandelten oder durch Akzeptieren von AGBs geschlossenen Vertrages. Demnach entspricht der Inhalt des *Smart Contracts* einer technischen Übersetzung des zwischen den Parteien vorher Vereinbarten und kann mit der rechtlichen Beurteilung eines Warenautomaten verglichen werden. Im Zusammenhang mit der Identitätsverwaltung könnte über die vorher vereinbarten Nutzungsbedingungen die Autorisierung der Komponenten im Internet der Dinge durch einen *Smart Contract* erfolgen. Damit könnte neben der Authentifikation und Identifikation des Nutzers beim Einsatz der Komponenten, die automatisierte Durchführung mehrerer Dienste in einem Kontext durch einen *Smart Contract* ermöglicht werden.

Schliesslich bedarf es über den im Algorithmus verkörperten Regelungsgehalt der Vertragsbedingungen jeweils keines Vertrauensvorschusses, denn mit dem *Smart Contract* wird die Gegenleistung «garantiert» über den Ausführungsmechanismus vorgenommen.[9]

2.2. Zentrales System

Als Gegenmodell zu der dezentralen Blockchain kommt die zentrale Steuerung der Datensätze in den Komponenten durch eine *Trusted Third Party* (TTP) in Betracht. Dabei stellt sich die grundsätzliche Frage, ob ein zentraler Vertrauensanker als staatliches oder privates System begründet wird. Die bestehenden Regelungen zum Signaturrecht über die eIDAS-Verordnung, die österreichische Bürgerkarte oder der deutsche elektro-

---

2 Sog. «*distributed digital ledger*».

3 IEEE, Spectrum, 10/2017, Blockchains: How they work and why the will change the world, S. 25–28. Danach wird zunächst auf Bitcoin Bezug genommen mit einem Ausblick auf weitere Anwendungen etwa den Kontext *Social Media*.

4 IEEE, Spectrum, 10/2017 (Fn. 3), S. 32–33. Hinsichtlich der hohen Rechenleistung und des Energieverbrauches werden daher Alternativen diskutiert, etwa «Hashgraph».

5 IEEE, Spectrum, 10/2017 (Fn. 3), S. 27; Wattenhofer (Fn. 1), S. 83: Definition: PoW is a mechanism that allows a party to prove to another party that a certain amount of computation resources has been utilized for a period of time.

6 Kaulartz/Heckmann, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, S. 618–619.

7 Definition: Smart Contract is an agreement between two or more parties, encoded in such a way that the correct execution is guaranteed by the blockchain. Aus wattenhofer (Fn. 1), S. 87.

8 Wattenhofer (Fn. 1), S. 89

9 Vgl. Kaulartz/Heckmann, Smart Contracts (Fn. 6), S. 618–622; Kaulartz/Heckmann, Smart Dispute Resolution, DSRI 2017, S. 599, 603

nische Personalausweis[10] sind Beispiele für ein zentrales staatliches System von Vertrauensankern, sog. *E-Government*. Demgegenüber stehen Systeme von privaten Anbietern, die *Single Sign On*-Lösungen vorsehen. Dabei stellt sich die Frage nach Verknüpfungen, bei denen eine private Blockchain über eine Schnittstelle zu einem anderen etwa zentralen TTP System verfügt, welches ein übergeordnetes und interoperables Konzept einer Identitätsverwaltung im Sinne des Rechts auf Datenportabilität nach Art. 20 DSGVO verkörpern könnte.

3. Rechtliche Anforderungen bei der Identitätsverwaltung

Bezüglich der kontextspezifischen Anforderungen an ein dezentrales System und an ein zentrales System sollen folgend die datenschutzrechtliche (3.1.) und die signaturrechtliche Betrachtung mit einem Bezug zum ISAEN-Konzept (3.2.) vorgenommen werden.

3.1. Datenschutzrechtliche Betrachtungen

3.1.1. Personenbezogene Daten

Im Internet der Dinge ist der datenschutzrechtliche Anwendungsbereich eröffnet, wenn die Datenverarbeitung personenbezogene Daten umfasst (Art. 4 Nr. 1 DSGVO). In Abgrenzung zu Sachdaten liegen personenbezogene Daten vor, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, was mitunter mittels Zuordnung zu einer Kennung, Standortdaten oder einem Identifizierungsmerkmal möglich ist.[11] Nicht erfasst sind demnach anonymisierte Datensätze, so dass bei einer rechtlich anerkannten Anonymisierungsmethode der Anwendungsbereich des Datenschutzes nicht eröffnet ist. Hierbei kommen als Anonymisierungsmethoden insbesondere *Differential Privacy* und *Pufferfish Framework* in Betracht.[12]

Sobald für ein Identitätsverwaltungskonzept die Steuerung der kontextbezogenen Datensätze über die Blockchain erfolgen würde, stellt sich die Frage nach der Zuordnung des Hashwertes als personenbezogenes Datum.[13] Dabei kommt im Hashwert ein hohes Verschlüsselungsmaß zum Ausdruck, was die Annahme eines anonymen Datensatzes wegen der kaum möglichen Rückrechnung auf den Ursprungsdatensatz rechtfertigen kann.[14]

3.1.2. Datenminimierung

Der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 c) DSGVO verlangt, dass die Verarbeitung der personenbezogenen Daten dem Zweck angemessen und auf das notwendige Maß beschränkt wird. Dabei ist für ein Identitätsverwaltungskonzept im Internet der Dinge maßgeblich, dass die technische Gestaltung kontextspezifische Vertrauens- und Sicherheitsmaße mit dem Einsatz von Anonymisierungs-, Pseudonymisierungs-[15] und Verschlüsselungstechniken umfasst. Gleichzeitig stellt sich bei der Blockchain die Frage, ob die Datenminimierung realisiert werden kann. Denn sobald personenbezogene Daten in der Blockchain hinterlegt sind, besteht eine vielfache dezentrale Speicherung und es liegt gerade keine Beschränkung der Speicherung auf das notwendige Maß vor.

3.1.3. Automatisierte Einwilligung?

Die Verarbeitung personenbezogener Daten im Internet der Dinge müsste rechtmäßig sein, Art. 6 Abs. 1 DSGVO. Dabei kommt die Rechtmäßigkeit insbesondere über Erforderlichkeit, das berechtigte Interesse der

---

10 §§ 10, 18, 19 deutsches PAuswG oder die E-ID als Bürgerkarte in Österreich.

11 Erwägungsgründe 26, 27, 30, 31 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutz-Grundverordnung; DSGVO).

12 Buchmann, Wie kann man Privatheit messen?, DuD 2015, S. 510–514.

13 Vgl. Voitel, Sind Hashwerte personenbezogene Daten?, DuD 2017, S. 686.

14 Smart Data – Begleitforschung, Sicheres Identitätsmanagement im Internet, Berlin 2017, S. 34. https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smartdata_studie_isaen.pdf (alle Websites zuletzt besucht am 16. Januar 2019).

15 Art. 4 Nr. 5 DSGVO.

Datenverarbeitung und die Erteilung einer Einwilligung in Betracht, Art. 6 Abs. 1 a), c), f) DSGVO. Zwar lässt sich die Rechtmäßigkeit im Internet der Dinge über die Erforderlichkeit für die Durchführung eines Vertrages und das berechtigte Interesse der verantwortlichen Stelle und eines Dritten ableiten, jedoch soll an dieser Stelle die Einwilligung als Mittel der Kontrolle über die Datenverarbeitung und Ausübungsmöglichkeit des Rechts auf informationelle Selbstbestimmung im Vordergrund stehen.

Indem bei einem Identitätsverwaltungssystem über die Komponenten des Internets der Dinge die Herstellung der Funktionalität durch *Smart Contracts* in Betracht kommt, könnte etwa im Kontext des *Smarten Arbeitsplatzes* oder des *Smart Home* ein «*general consent*»[16] erteilt werden. Dabei bedürfte es eines elektronischen Zeitstempels[17] über den Zeitpunkt der erteilten Einwilligung, die etwa über ein *Dashboardsystem*[18] oder in einer Blockchain einzusehen wäre, womit eine Kontrollmöglichkeit gewährleistet wäre.

3.1.4. Betroffenenrechte

Ein maßgeblicher Schutzmechanismus in einem Identitätsverwaltungssystem sind die Betroffenenrechte nach Art. 15–21 DSGVO. In einem Konzept der Identitätsverwaltung sind gerade die Berichtigung der Datensätze, Art. 16 DSGVO, die Löschung der Datensätze, Art. 17 DSGVO, oder die Übertragung dieser, Art. 20 DSGVO, als Betroffenenrechte maßgeblich für die nachträgliche Realisierung des Rechts auf informationelle Selbstbestimmung. Dabei sind das Recht auf Datenübertragbarkeit und das Recht auf Löschung der Datensätze Person besonders geeignet, die Datensätze zu kontrollieren und die Identitäten zu verwalten. Das Recht auf Datenübertragbarkeit ermöglicht in einem strukturierten Verfahren den erleichterten Anbieterwechsel und die Wiederverwendung einmal erhobener Daten.[19] Dies könnte etwa bei dem Wechsel eines Dienstanbieters, der Universität[20] oder dem *Smarten Arbeitsplatz* erforderlich sein. Gleichzeitig stellt sich die Problematik, dass gemäß Art. 20 Abs. 1 DSGVO nur solche Datensätze erfasst sind, die «bereitgestellt» wurden. Damit sind Kommunikationsdaten mit Dritten oder erstellte Profile nicht ohne weiteres von dem Anwendungsbereich des Art. 20 DSGVO erfasst.[21] Zur Verwaltung der identitätsbezogenen Datensätze kommt daher ein Tool in Betracht, mit dem die Übertragung von kontextspezifischen Datensätzen ermöglicht wird und diese Datensätze hinterlegt werden könnten.

Als weiteres Recht sieht das Recht auf Löschung der Datensätze nach Art. 17 DSGVO vor, dass die betroffene Person durch die Löschung der sie betreffenden Datensätze ihr Recht auf informationelle Selbstbestimmung in Zeiten von *Big Data* substantiell ausüben kann. Beim Einsatz von Komponenten im Internet der Dinge und damit entstandenen Profilen könnte der Bedarf nach einem Neuanfang über das entstandene Profil entstehen, welcher mit dem sog. «Recht auf Vergessenwerden»[22] ausgeübt werden könnte. Gleichzeitig kann mit der Ausübung des Rechts und der Löschung der Datensätze ein eigenständiger Informationsgehalt über die betroffene Person entstehen, so dass neben der Löschung der Datensätze die Einstellung der betroffenen Person zur konkreten Datenverarbeitung erkennbar wird.[23] Insgesamt stelle das Recht auf Löschung der Datensätze ein unzureichendes Kontrollmittel über die Datensätze in Anbetracht der Ubiquität von Datenverarbeitungsprozessen dar.[24] Insoweit kommt als kompensatorisches Mittel die Gestaltung eines Identitätsverwaltungskonzeptes

16 https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/telephone-marketing/.

17 Vgl. Jandt/Schaar/Schulz, Beck TMG Kommentar, München 2013, § 13 TMG Rn. 76.

18 Raschke/Küpper/Drozd/Kirrane, Designing a GDPR-compliant and usable Privacy Dashboard, S. 10–12; https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

19 Art. 29 Data protection working party, Guidelines on the right to data portability, WP 242 rev. 1, S. 5.

20 Vgl. Janal, Data Portability – A Tale of Two Concepts, Jipitec 2017, S. 5 f.

21 Janal, Data Portability – A Tale of Two Concepts, Jipitec 2017, S. 3; Art. 29 Data protection working party, Guidelines on the right to data portability, WP 242 rev. 1, S. 9.

22 Vgl. Google Spain SL / Gonzales, EuGH 13. Mai 2014, C-131/12.

23 Spiecker gen. Döhmann, Steuerung im Datenschutzrecht – Ein Recht auf Vergessen wider Vollzugsdefizite und Typisierung, KritV 2014, S. 28, 35

24 Drackert, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 71, Fn. 267.

mit differenzierten Anonymisierungs- und Pseudonymisierungsmethoden in Frage, welches im Gleichlauf mit dem Grundsatz der Datenminimierung stünde.

Schließlich erscheint unter Anwendung der Blockchain die Umsetzung der Betroffenenrechte erschwert, indem die Speicherung der Datensätze dezentral erfolgt und irreversibel ist. Das Recht auf Berichtigung von Daten und das Recht auf Vergessenwerden kann daher nicht anforderungsgemäß umgesetzt werden. Allenfalls kommt als Separierung das *Forking* in Betracht, welches jedoch zu einer Gabelung der Blockchain führt und nicht zu einer inhaltlichen Berichtigung oder Löschung der Datensätze. So könnte der Einsatz von Assistenzsystemen als Komponenten im Internet der Dinge am *Smarten Arbeitsplatz* den Bedarf auslösen, dass Datensätze zu einem Arbeitnehmer nach der Zweckerreichung gelöscht werden oder das Recht auf Vergessenwerden nach Art. 17 DSGVO geltend gemacht wird.

3.2. Signaturrechtliche Betrachtungen

Die eIDAS-Verordnung[25] sieht grundsätzlich eine zentrale Vertrauensinstanz vor, mit der im behördlichen und privaten Kontext[26] drei verschiedene Ebenen für das Vertrauensniveau der Identifizierung eingesetzt werden können, Art. 8 eIDAS-VO. Insofern können die Vorgaben der eIDAS-Verordnung nach dem ISAEN-Konzept[27] herangezogen werden, wonach mit dem Einsatz der Blockchain als vertrauenswürdigen Intermediär die Bestätigung der Einwilligung in einem Hashwert erfolgen könnte.[28] Bei diesen Identifizierungsverfahren wird eine bestimmte Menge an Identitätsattributen («identifier») bei dem Nutzer gespeichert («safe») und zur Sicherung mit einer elektronischen Signatur und einem elektronischen Zeitstempel versehen, was in einen Hashwert generiert wird («ISAEN-App»).[29] Dieser würde die Protokollierung der datenschutzrechtlichen Einwilligung umfassen können mit der jederzeit nachvollziehbar wäre, ob und wann eine Einwilligung für die kontextbezogene Datenverarbeitung erteilt wurde.[30]

Insgesamt kann das Sicherheits- und Vertrauensmaß des Identifizierungsmittels nach Art. 8 eIDAS-VO in «niedrig», «substantiell» und «hoch» eingestuft werden, was eine kontextangemessene Verwaltung der Datensätze ermöglichen würde. Dabei wäre ein hohes Vertrauensmaß im Kontext des *E-Government* erforderlich, womit ein Vertrauensanker für entsprechende Kontexte mit einem vergleichbar hohen Vertrauensbedarf wie etwa *E-Health* gebildet werden könnte.[31] Dafür wäre die Blockchain zur Begründung dieses Vertrauensankers geeignet, solange die personenbezogenen Datensätze selbst nicht in der Blockhain gespeichert werden würden. Sobald jedoch gesundheitsrelevante Daten in der Blockchain hinterlegt werden müssten, erscheint ein zentraler Vertrauensanker naheliegend. Demgegenüber könnte der Kontext des *Smart Homes* und die Verwendung von *Wearables* mit einem geringeren Vertrauens- und Sicherheitsmaß ausgestaltet werden, sog. «*Identity Ecosystem*».[32]

---

25 Verordnung (EU) 910/2014 des europäischen Parlaments und Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

26 Erwägungsgrund 17 eIDAS-VO.

27 Smart Data – Begleitforschung (Fn. 14), S. 29 ff.

28 Smart Data – Begleitforschung (Fn. 14), S. 4–7.

29 Art. 3 Nr. 33 eIDAS-VO: «Elektronischer Zeitstempel» bezeichnet 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.

30 Smart Data – Begleitforschung (Fn. 14), S. 29 ff.

31 The White House, National Strategy for trusted identities in cyberspace, Enhancing online choice, Efficiency, Security, and Privacy, April 2011, S. 17 f.

32 The White House, National Strategy for trusted identities in cyberspace, Enhancing online choice, Efficiency, Security, and Privacy, April 2011, S. 31–35.

3.2.1. Datenschutz durch Technikgestaltung

Gemäß Art. 25 Abs. 1 DSGVO soll der Stand der Technik für die wirksame Umsetzung der Datenschutzprinzipien durch die verantwortliche Stelle berücksichtigt werden. Hierbei stellt der Stand der Technik die rechtlich-technische Grundlage für die interdisziplinäre Ausfüllung der Konzepte *privacy by design* und *privacy by default* dar.[33] Diese verlangen bei einer Identitätsverwaltung im Internet der Dinge die technischen Methoden der Anonymisierung, Pseudonymisierung und Verschlüsselung angepasst auf das Schutzniveau in dem spezifischen Kontext. Ebenso wird die subjektive Perspektive der verantwortlichen Stelle einbezogen, indem diese den Stand der Technik aus dem konkreten Anwendungsfall heraus bestimmt, wie es sich aus dem Wortlaut «Berücksichtigung» gemäß Art. 25 Abs. 1 DSGVO ergibt.[34] Insofern würden die Maßnahmen zur Realisierung eines einheitlichen Schutzniveaus innerhalb des Internets der Dinge von den jeweils verantwortlichen Stellen unterschiedlich angesetzt werden und zudem kontextabhängig variieren.[35]

4. Ausblick

Die Kontrolle und Steuerung durch die Akteure im Internet der Dinge bedürfen eines Identitätsverwaltungssystems, was über die Einwilligung durch die natürliche Person vorgenommen werden kann und in der Schnittmenge zwischen dem Signatur- und Datenschutzrecht liegt.[36] Dabei kann die Blockchain aufgrund ihrer allgemeinen Transparenz und Sicherheit ein hohes Vertrauens- und Sicherheitsmaß gewährleisten. Gegenstand der Blockchain in einem Konzept der Identitätsverwaltung sollten daher nicht die personenbezogenen Daten sein, sondern die Autorisierung und Kontrolle der Datensätze in dem jeweiligen Kontext. Entsprechend könnte die Speicherung der Einwilligung nach dem ISAEN-Konzept eine Anknüpfung sein und zu einer kontextspezifischen Autorisierung von Komponenten über *Smart Contracts* führen. Die rechtlichen Anforderungen an die Umsetzung eines Identitätsverwaltungskonzeptes lassen sich aus Art. 8 eIDAS-VO und den Grundsätzen der DSGVO ableiten und sollten frühzeitig in die technische Gestaltung integriert werden (Art. 25 DSGVO). Aufgrund der hohen Interdependenz zwischen Mensch und Technik im Internet der Dinge ist besondere Aufmerksamkeit auf die technische Gestaltung im Hinblick auf *usability, privacy by design* und *privacy by default* zu setzen, so dass ein Konzept der Identitätsverwaltung mit der Pseudonymisierung, Verschlüsselung und Anonymisierung in ein datenschutzkonformes Konzept überführt werden könnte.

---

33 Erwägungsgrund 78.

34 Vgl. BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77, NJW 1979, S. 359, 362 – Kalkar I; Breuer, AöR 1976 (101). 46, 68.

35 Vgl. Schallbruch, Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste, CR 2016, 663 ff.

36 Art. 5 eIDAS-VO.