Datenschutzrechtliche Zulässigkeit der Übermittlung von Informationen über Migranten zwischen öffentlichen Stellen mittels einer Permissioned-Blockchain

Prof. Dr. Thomas Hoeren

Dipl. iur. Johannes Baur

A. Einführung

Bislang werden auf nationaler Ebene Informationen über Migranten, die von öffentlichen Stellen zur Erledigung ihrer Aufgaben benötigt werden, in einem vom Bundesamt für Migration und Flüchtlinge (BAMF) geführten Ausländerzentralregister (AZR) gespeichert. Öffentliche Stellen, die Informationen über Migranten erhalten, übermitteln diese, entsprechend den gesetzlichen Bestimmungen, an die Verwalter des AZR. Öffentliche Stellen, die Informationen über einen Migranten benötigen, erhalten, ebenfalls entsprechend gesetzlichen Bestimmungen, Auskunft über die benötigten Einträge im AZR. Dieses Verfahren soll durch eine direkte Übermittlung der Informationen zwischen den beteiligten öffentlichen Stellen vereinfacht werden.

I. Kurzbeschreibung des Vorhabens

Statt migrantenbezogene Informationen an zentraler Stelle zu speichern, sollen diese beim geplanten Vorhaben auf den lokalen Systemen der öffentlichen Stellen, welche die Informationen initial erhoben haben, belassen werden. Durch Vernetzung der öffentlichen Stellen untereinander mittels einer Permissioned-Blockchain soll der Datenaustausch zwischen den beteiligten öffentlichen Stellen direkt und ohne Umwege über eine Zentralstelle ermöglicht werden. Dabei soll die Permissioned-Blockchain zunächst auf der öffentlichen Ethereum-Blockchain aufgebaut werden. Öffentliche Stellen, die über neue Informationen über einen Migranten verfügen, veröffentlichen in der Permissioned-Blockchain einen neuen Eintrag („On-Chain-Datum"), welcher Grundinformationen über die Statusänderung und einen Verweis auf den Speicherort der Informationen („Off-Chain-Daten") auf dem lokalen System der öffentlichen Stelle enthält. Eintragungen in die Permissioned-Blockchain können nur von denjenigen Stellen vorgenommen werden, die durch ein zentral administriertes Rechte- und Rollensystem mit den notwendigen Schreiberechten ausgestattet wurden. Dieses System entscheidet auch darüber, welche öffentlichen Stellen an den jeweiligen Einträgen Leseberechtigungen erhalten. Auf diese Weise wird verhindert, dass Personen außerhalb der geschlossenen Nutzergruppe der öffentlichen Stellen Einsicht in die Daten gewinnen können. In einem ersten Pilotprojekt sind zunächst nur Aufnahmeeinrichtungen, das BAMF und die Ausländerbehörde Nürnberg beteiligt. Im späteren Verlauf sollen weitere öffentliche Stellen

hinzukommen. Eine Zukunftsvision ist die Ausweitung des Projekts auf weitere Mitgliedsstaaten der Europäischen Union.

II. Gang der Untersuchung

Im folgenden Gutachten soll die datenschutzrechtliche Zulässigkeit des soeben beschriebenen Vorhabens untersucht werden. Es ist dabei davon auszugehen, dass die initiale Erhebung und Erfassung von personenbezogenen Daten durch die öffentlichen Stellen bei den betroffenen Migranten rechtlich zulässig ist. Die Untersuchung soll sich daher auf die Zulässigkeit des Austausches der bereits erhobenen Informationen zwischen den öffentlichen Stellen beschränken. Im Vordergrund steht hierbei die Vereinbarkeit des Vorhabens mit den Vorschriften der EU-Datenschutz-Grundverordnung (DS-GVO).

In einem ersten Schritt wird geprüft, an welchen Stellen es beim geplanten Vorhaben zu Datenverarbeitungen kommt (B.I.), ob es sich bei den verarbeiteten Daten um personenbezogene Daten handelt (B.II.) und wer Verantwortlicher für die jeweilige Datenverarbeitung ist (B.III.).

Im zweiten Schritt wird die Rechtfertigung dieser Datenverarbeitungen geprüft (C.), wobei sich auf Art. 6 Abs. 1 DS-GVO und insbesondere auf Art. 6 Abs. 1 lit. e DS-GVO gestützt wird. Die hierfür erforderlichen zusätzlichen nationalen Rechtsgrundlagen werden diskutiert. Eine Prüfung der Erforderlichkeit der Datenübermittlung für die Erledigung der Aufgaben der jeweils beteiligten öffentlichen Stellen in Bezug auf die im Einzelnen übertragenen Daten erfolgt dabei nicht.

In einem weiteren Schritt werden im geplanten Vorhaben voraussichtlich zu verarbeitende sensible Daten nach Art. 9 DS-GVO identifiziert (D.I.). Da deren Verarbeitung grundsätzlich unzulässig ist, werden Ausnahmevorschriften geprüft (D.II.). Dabei wird insbesondere auf die Datenverarbeitung zu Archivzwecken im öffentlichen Interesse, wissenschaftlichen Forschungszwecken und statistischen Zwecken, sowie auf die Verarbeitung im erheblichen öffentlichen Interesse eingegangen.

Im nächsten Schritt wird überprüft, inwieweit sich die Betroffenenrechte der Art. 12 ff. DS-GVO durch das geplante Blockchain-Vorhaben umsetzen lassen (E.). Dabei wird neben dem Informations- und Auskunftsrecht auch das Recht auf Vervollständigung angesprochen und

untersucht, ob es sich um automatisierte Entscheidungen im Einzelfall nach Art. 22 DS-GVO handelt. Im Zentrum des Interesses steht jedoch die Umsetzung des Rechts auf Berichtigung falscher und Löschung nicht mehr erforderlicher Daten.

Im letzten Schritt soll lfestgestellt werden, inwieweit technische und organisatorische Maßnahmen zur Wahrung der Datenschutzgrundsätze nach Art. 25 DS-GVO ergriffen werden können (F.). Dabei sollen zunächst die Risiken der geplanten Datenverarbeitungen für die Rechte und Freiheiten der betroffenen Personen beleuchtet werden. Zuletzt wird auf konkrete Maßnahmen zur Wahrung der Datenschutzgrundsätze eingegangen.

B. Verarbeitung personenbezogener Daten

Nach Art. 1 Abs. 2 DS-GVO ist der Zweck der Datenschutz-Grundverordnung der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere des Rechts auf Schutz personenbezogener Daten. Verarbeitungen von Daten sind daher nicht im Allgemeinen datenschutzrechtlich relevant, sondern nur dann, wenn es sich um „personenbezogene Daten" handelt.[1]

Zu prüfen ist, ob und an welchen Stellen es beim konkreten Vorhaben der Übermittlung von Daten zwischen den beteiligten öffentlichen Stellen zu einer Verarbeitung von personenbezogenen Daten kommt. Zunächst soll dabei festgestellt werden, welche Datenverarbeitungen im konkreten Fall für die Untersuchung relevant sind. Weiter wird geprüft, ob die dabei verarbeiteten Daten einen Personenbezug aufweisen und wer Verantwortlicher für die Datenverarbeitung ist.

I. Relevante Datenverarbeitungen

Der Begriff der Datenverarbeitung nach der DS-GVO ist weit gefasst. Art. 4 Nr. 2 DS-GVO enthält eine Legaldefinition, wonach „jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe, wie das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung" von Daten als eine Datenverarbeitung anzusehen ist.

1. Einpflegung der Daten in die Blockchain

Die erste relevante Handlung ist die Einpflegung der Daten in die Blockchain durch die weitergebende öffentliche Stelle. Dabei bleiben die weiterzugebenden Daten größtenteils lokal auf dem System der weitergebenden öffentlichen Stelle gespeichert. Durch einen Verweis, der in der Blockchain abgelegt wird, werden die Daten anderen öffentlichen Stellen mit Lesezugriff zugänglich gemacht. Diese Form der Zugänglichmachung könnte als eine Offenle-

---

1 So auch Ehmann/Selmayr/*Klabunde*, EU-DS-GVO, 1. Aufl. 2017, Art. 4, Rn. 5; Sydow/*Ziebarth*, EU-DSGVO, 1. Aufl. 2017, Art. 4, Rn. 9; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 4.

gung durch Übermittlung oder eine Verbreitung angesehen werden, wenigstens jedoch ist sie als „andere Form der Bereitstellung" an die öffentlichen Stellen mit Lesezugriff zu qualifizieren, sodass von einer Datenverarbeitung auszugehen ist.

Zusätzlich zum Verweis auf die lokal gespeicherten Daten sollen in die Blockchain eine Kennnummer des Migranten, der aktuelle Status, die bearbeitende öffentliche Stelle und ein Zeitstempel gespeichert werden. Diese Daten sind ebenfalls für alle öffentlichen Stellen mit Lesezugriff einsehbar. Insofern handelt es sich um eine Offenlegung durch Übermittlung.[2]

2. Weiterverarbeitung der Daten in der Blockchain

Die in den Blöcken eingespeicherten Daten werden durch die Nodes der Blockchain fortlaufend gespeichert und je nach Systemarchitektur der Blockchain von Minern weiterverarbeitet. Diese Handlungen sind als „Organisation", „Ordnen" oder „Speichern" von Daten ebenfalls Datenverarbeitungen.

3. Auslesen der Daten aus der Blockchain

Öffentliche Stellen mit Lesezugriff erhalten die Möglichkeit, die in die Blockchain eingespeicherten Daten auszulesen. Von diesen Daten sind auch die über den Verweis zugänglichen Off-Chain-Daten umfasst. Diese Auslesevorgänge sind ebenfalls Datenverarbeitungen.

II. Personenbezug der verarbeiteten Daten

Bei den verarbeiteten Daten müsste es sich um „personenbezogene Daten" handeln. Der Begriff ist in Art. 4 Nr. 1 S. 1 DS-GVO legaldefiniert. Demnach sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Der Begriff des personenbezogenen Datums war bereits Gegenstand der EU-Richtlinie 95/46/EG (Datenschutzrichtlinie) und wurde von der Artikel-29-Datenschutzgruppe näher untersucht.[3] Ein personenbezogenes Datum besteht demnach aus den vier Elementen

---

2 Ebenso für eine Public-Blockchain, *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, Informatik 2017, 1025 (1033).

3 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten".

natürliche Person, Information, Personenbezug und Identifizierung bzw. Identifizierbarkeit. Dies lässt sich für die Auslegung des Begriffs nach der DS-GVO übertragen.[4]

1. Natürliche Person

Von der DS-GVO sind nur die Daten natürlicher Personen geschützt. Zu den natürlichen Personen zählen alle Menschen ungeachtet ihrer Staatsangehörigkeit. Erfasst sind aber nur lebende Personen, nicht Daten Verstorbener.[5] Die Mitgliedsstaaten können jedoch zum Schutz dieser Daten eigene Regelungen treffen. Zu beachten ist, dass ein Datum, das sich auf eine verstorbene Person bezieht, gleichzeitig auch Informationen über noch lebende Personen enthalten kann.[6]

Bei den registrierten Migranten handelt es sich um natürliche Personen. Es ist auch davon auszugehen, dass es sich bei diesen um lebende Personen handelt. Informationen über die verarbeitenden öffentlichen Stellen sind hingegen datenschutzrechtlich nicht relevant. Etwas anderes gilt nur dann, wenn auch Daten verarbeitet werden, die Informationen über konkrete Angestellte der öffentlichen Stelle enthalten.

2. Information

Der Begriff der „Information" ist weit gefasst und enthält sowohl objektive Informationen (z.B. Name, Wohnort) sowie subjektive Informationen (z.B. Meinungen, Äußerungen). Der Wahrheitsgehalt der Information spielt dabei keine Rolle. Die Information kann in jedem erdenklichen Format vorliegen.[7]

Nahezu alle Daten, die im geplanten Blockchain-Verfahren verarbeitet werden, haben einen mehr oder weniger großen Informationsgehalt. Dies gilt nicht nur für die Off-Chain-Daten, sondern auch für on-chain gespeicherte Kennnummer, den Status, die bearbeitende öffentliche Stelle und den Zeitstempel.

---

4 Ebenso Ehmann/Selmayr/*Klabunde*, EU-DS-GVO, 1. Aufl. 2017, Art. 4, Rn. 6.

5 DS-GVO, Erwägungsgrund 27.

6 BeckOK DatenschutzR/*Schild*, DS-GVO, 23. Ed., Art. 4, Rn. 11; *Kühling*/Buchner/*Klar*, DS-GVO, 2. Aufl. 2018, Art. 4, Rn. 5; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 26.

7 Ehmann/Selmayr/*Klabunde*, EU-DS-GVO, 1. Aufl. 2017, Art. 4, Rn. 7; Sydow/*Ziebarth*, EU-DSGVO, 1. Aufl. 2017, Art. 4, Rn. 41.

Eine Information ist den Daten jedoch nur dann zu entnehmen, wenn diese für den Betrachter auch lesbar ist. Diese Möglichkeit haben nur diejenigen, die vom System mit einem Leserecht ausgestattet sind. Alle anderen Beteiligten können die Daten zwar ebenfalls in der Blockchain begutachten, aufgrund der Verschlüsselung können sie diesen aber keinen Informationsgehalt über natürliche Personen entnehmen. Für Personen ohne Lesezugriff handelt es sich folglich nicht um personenbezogene Daten.[8] Dies gilt nicht nur für die an der Permissioned-Blockchain teilnehmenden öffentlichen Stellen, denen für den konkreten Blockchain-Eintrag der Lesezugriff fehlt, sondern auch für alle Nodes und Miner der zugrundeliegenden Public-Blockchain.[9] Diese verarbeiten lediglich Daten ohne Informationsgehalt. Für diese stellen die Daten daher bereits aus diesem Grund keine personenbezogenen Daten dar.

3. Personenbezug

Nach Ansicht der Artikel-29-Datenschutzgruppe besteht ein Personenbezug dann, wenn entweder ein Inhaltselement oder ein Zweckelement oder ein Ergebniselement vorhanden ist. Ein Inhaltselement liegt vor, wenn es sich bei den Informationen um solche über die Person handelt, ein Zweckelement dann, wenn sie „mit dem Zweck verwendet werden bzw. verwendet werden können, um eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen"[10]. Ein Ergebniselement liegt vor, wenn sich die Information auf die Rechte und die Interessen einer bestimmten Person auswirken könnte. Es genügt dabei, wenn die Person aufgrund der Verarbeitung der In-

---

8 So auch *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 23, welche deutlich macht, dass keine personenbezogenen Daten vorliegen, wenn durch technische Maßnahmen die Herstellung einer Information ausgeschlossen ist. Diese Differenzierung nimmt der Blockchain Bundesverband nicht vor, indem er pauschal behauptet, dass es sich bei verschlüsselten Daten um pseudonymisierte Daten handelt, ***Blockchain Bundesverband***, Blockchain, data protection and the GDPR, v.1.0, 25.05.2018, S.4, abrufbar unter: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf (zuletzt abgerufen am: 15.06.2018).

9 ***Martini/Weinzierl***, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1254), sehen Nodes und Miner in einer zulassungsbeschränkten Blockchain als Auftragsverarbeiter. Sie gehen dabei jedoch nicht auf den hier entscheidenden Umstand ein, dass die Daten verschlüsselt sind.

10 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 11 f.

formation anders behandelt werden könnte als andere Personen.[11] Bei der Untersuchung aller Elemente müssen stets die näheren Begleitumstände des Einzelfalls Beachtung finden.

Betrachtet man zunächst die Off-Chain-Daten, so wird deutlich, dass es sich hierbei um Informationen über den konkreten Migranten handelt (Inhaltselement). Der Zweck der Verarbeitung besteht sogar darin, den Migranten aufgrund der Informationen unterschiedlich zu behandeln (Zweckelement). Dies wirkt sich auf die Rechte und Interessen des Migranten aus (Ergebniselement). Gleiches gilt jedoch ebenso für die On-Chain-Daten. Daten über den Status, die Behörde und der Zeitstempel enthalten in gleicher Weise Informationen über den betroffenen Migranten. Folglich enthalten sowohl On-Chain- als auch Off-Chain-Daten Informationen über eine Person.

4. Identifizierung oder Identifizierbarkeit

Identifiziert ist eine Person dann, wenn sie sich in einer Personengruppe von allen Personen unterscheidet.[12] Nach Art. 4 Nr. 1 S. 2 DS-GVO ist eine Person identifizierbar, wenn sie 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. Für die Frage, ob eine Person identifizierbar ist, kommt es immer auf die konkreten Umstände des Einzelfalls an. Dabei sollten nach Erwägungsgrund 26 der DS-GVO alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Der EuGH hat dies in der Rechtsprechung zum Personenbezug dynamischer IP-Adressen dahingehend präzisiert, dass ein personenbezogenes Datum für den Verarbeitenden dann vorliegt, wenn dieser entweder selbst über alle erforderlichen Informationen zur Identifikation verfügt oder zumindest über rechtliche Mittel verfügt, um diese Informationen von Dritten zu erlangen.[13]

---

11 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 13.
12 Ebd., S. 14.
13 EuGH, Urteil vom 19.10.2016 - C-582/14, Rn. 49.

a) Direkte Identifikation im Blockchain-Verfahren

Eine direkte Identifikation einer Person erfolgt in der Regel durch Kenntnis von deren Namen.[14] Da dieser jedoch nicht einmalig ist, bedarf es für eine eindeutige Identifikation weiterer Informationen, wie beispielsweise dem Geburtsdatum, einem Lichtbild oder einer Adresse.[15]

Betrachtet man Off-Chain- und On-Chain-Daten in ihrer Gesamtheit, so ist eine direkte Identifizierung problemlos möglich. Die Grundpersonalien nach § 3 Abs. 1 Nr. 4 AZRG erlauben eine eindeutige Zuordnung des Migranten.

b) Indirekte Identifikation durch die Kennnummer

Ohne die Off-Chain-Daten ist die direkte Identifizierung des Migranten nicht mehr möglich. Eine indirekte Identifizierung ist hingegen auch dann möglich, wenn eine „einzigartige Kombination"[16] an Informationen vorliegt, die in ihrer Gesamtheit nur auf eine bestimmte natürliche Person zutreffen kann, obwohl die einzelnen Informationen noch keine Rückschlüsse erlauben. Hierzu zählen auch die von Art. 4 Nr. 1 S. 2 DS-GVO genannten besonderen Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sind. Je dichter der Datensatz an Informationen über die Person, desto wahrscheinlicher wird deren Identifizierbarkeit. Die Kenntnis des Namens der Person ist dabei keine zwingende Voraussetzung[17].

Betrachtet man nur die On-Chain-Daten, so enthält der Datensatz weiterhin die Information, dass zu einer bestimmten Kennnummer von einer bestimmten öffentlichen Stelle zu einem bestimmten Zeitpunkt ein bestimmter Status des Migranten eingetragen wurde. Solange der Verarbeitende oder ein Dritter die Information darüber hat, welche natürliche Person sich hinter der gespeicherten Kennnummer verbirgt, ist der Personenbezug herstellbar. Auch wenn ein Zugriff auf die Off-Chain-Daten nicht (mehr) möglich ist, so sind die in der Block-

---

14 BeckOK DatenschutzR/*Schild*, DS-GVO, 23. Ed., Art. 4, Rn. 16; Sydow/*Ziebarth*, EU-DSGVO, 1. Aufl. 2017, Art. 4, Rn. 14.

15 BeckOK DatenschutzR/*Schild*, DS-GVO, 23. Ed., Art. 4, Rn. 16; Kühling/Buchner/*Klar*, DS-GVO, 2. Aufl. 2018, Art. 4, Rn. 18.

16 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 16.

17 BeckOK DatenschutzR/*Schild*, DS-GVO, 23. Ed., Art. 4, Rn. 16; Sydow/*Ziebarth*, EU-DSGVO, 1. Aufl. 2017, Art. 4, Rn. 17, 21.

chain eingespeicherten Daten personenbezogene Daten des Migranten, soweit der Schlüssel, mit welchem sich eine Verbindung zwischen natürlicher Person und Kennnummer herstellen lässt, für den Verarbeitenden (auch über Dritte) erreichbar bleibt.

Ist mangels Schlüssels die Herstellung einer Verbindung zwischen dem Migranten und der Kennnummer nicht (mehr) möglich, so käme eine indirekte Identifizierung des Migranten allein anhand der Off-Chain-Daten auch dadurch in Betracht, dass durch eine Zusammenschau aller in der Blockchain eingetragenen Statusänderungen nur ein Migrant für diese einzigartige Kombination infrage kommt. Da jedoch durch eine öffentliche Stelle mehrere Migranten mit demselben Status verarbeitet werden, wäre dieser Rückschluss nur durch genaue Analyse der Zeitstempel und Einbeziehung zusätzlicher Informationen des Verarbeitenden möglich. Bleiben die Daten in der Blockchain unveränderbar dauerhaft gespeichert, so muss dieses Risiko jedoch beachtet und entsprechende Vorkehrungen getroffen werden. Eine Lösung für diese Problematik könnte eine weitere Reduzierung der in der Blockchain eingespeicherten Daten sein.[18]

III. Verantwortlicher für die Datenverarbeitung

Adressat der Pflichten aus der DS-GVO ist grundsätzlich der für die Verarbeitung der Daten Verantwortliche.[19] Nur dieser wird durch eine Rechtsgrundlage zur Datenverarbeitung legitimiert. Aus diesen Gründen ist die Feststellung des Verantwortlichen von besonderer Bedeutung. Dabei ist neben der alleinigen Verantwortlichkeit einer Stelle auch eine geteilte Verantwortlichkeit mehrerer Stellen nach Art. 26 DS-GVO möglich. Der Verantwortliche kann sich zudem Auftragsverarbeitern (Art. 28 DS-GVO), die nach Weisung des Verantwortlichen tätig werden, bedienen.

Bei der Einpflegung von Daten in die Blockchain und beim Auslesen dieser Daten werden in erster Linie die jeweils beteiligten öffentlichen Stellen tätig. Die Weiterverarbeitung der Daten erfolgt dezentral ohne Einflussmöglichkeit der öffentlichen Stellen. Die Software, welche als Schnittstelle zwischen den Systemen der öffentlichen Stellen und der Blockchain den Datenaustausch ermöglicht, wird von zentraler Stelle bereitgestellt. Als zentrale Stelle (Zentralstelle) ist hier zunächst an das Bundesamt für Migration und Flüchtlinge, als den Initiator des

---

18 Siehe hierzu unter E.III.3.

19 Sydow/*Raschauer*, EU-DSGVO, 1. Aufl. 2017, Art. 4, Rn. 114.

Projekts, zu denken. Für zukünftige europäische Entwicklungen ist auch eine Koordination auf supranationaler Ebene denkbar. Es ist sowohl für die Einpflegung von Daten in die Blockchain als auch für das Auslesen dieser Daten jeweils zu prüfen, wie die Verantwortlichkeit zwischen den genannten Beteiligten verteilt ist.

1. Begriff der Verantwortlichkeit

Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für die Frage, wer „entscheidet", kommt es darauf an, wer tatsächlichen Einfluss auf die Entscheidung nimmt. Einer formalen rechtlichen Benennung eines Entscheidungsträgers kommt dabei nur Indizwirkung zu.[20]

Mit der Entscheidung über den Zweck ist diejenige über das erwartete oder geplante Ergebnis der Verarbeitung gemeint, die Entscheidung über die Mittel ist diejenige über die Art und Weise, wie dieses Ergebnis erreicht wird.[21] Der Begriff des Mittels umfasst dabei u.a. die Entscheidung über die technischen Methoden und den Umfang der Verarbeitung, die Zugangsberechtigung zu den Daten oder die Löschfristen.[22]

2. Verantwortlicher für das Auslesen der Daten

Beim Auslesen der Daten entscheidet allein die auslesende öffentliche Stelle darüber, ob und welche Daten ausgelesen werden. Folglich ist es alleine sie, die über Zwecke und Mittel der Datenverarbeitung entscheidet. Für die Verarbeitung des Auslesens ist sie die alleinige Verantwortliche für die Datenverarbeitung.

3. Verantwortlicher für die Einpflegung und Übermittlung der Daten

Schwieriger ist die Frage für die Einpflegung und Übermittlung der Daten zu beantworten. Im Folgenden soll zunächst eine mögliche Verantwortlichkeit der Nodes der Ethereum-

---

20 *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 15.

21 Ebd., S. 16.

22 Ebd., S. 17.

Blockchain ausgeschlossen werden. Im Anschluss wird die Verteilung der Verantwortlichkeit zwischen den Beteiligten der geplanten Permissioned-Blockchain untersucht.

a) Die Rolle der Nodes in der Ethereum-Blockchain

Für On-Chain-Daten wird teilweise angenommen, dass die Nodes der Blockchain als Verantwortliche oder zumindest als Auftragsverarbeiter tätig werden.[23] Dies beträfe im hier betrachteten Projekt die Nodes der Ethereum-Blockchain. Wie oben dargestellt, handelt es sich bei den verarbeiteten Daten aus der Perspektive der Nodes jedoch, aufgrund der Verschlüsselung, nicht um personenbezogene Daten. [24] Die Nodes folgen bei der Verarbeitung der Daten lediglich den Regeln des Blockchain-Systems und nehmen keinen Einfluss auf Mittel und Zwecke der Verarbeitung. Folglich können sie nicht als Verantwortliche für die Datenverarbeitung angesehen werden.

Eine Auftragsverarbeitung durch die Nodes würde eine Verarbeitung auf Weisung der Zentralstelle oder der am Projekt beteiligten öffentlichen Stelle voraussetzen. Tatsächlich haben die Nodes aber nicht einmal Kenntnis vom geplanten Projekt und den beteiligten Stellen. Sie sind lediglich als unbeteiligte Datenmittler tätig und handeln vollständig autark. Datenverarbeitungen durch Unbeteiligte sind im Internet gewöhnlich: bei jeder Kommunikation zweier Server über das Internet werden verschlüsselte Daten zwischen Sender und Empfänger durch unzählige Dritte weitertransportiert. Diesen Datenmittlern wird man jedoch schwerlich die Rolle von Auftragsverarbeitern, die nach Weisung der kommunizierenden Parteien tätig werden, zuschreiben können. Ähnlich wie die Gesamtheit der im Internet vernetzten Server die Kommunikation zwischen einzelnen Parteien ermöglicht, stellen die Nodes der Ethereum-Blockchain ein System bereit, dass von jedermann – auch für die Implementierung einer darauf aufbauenden Permissioned-Blockchain, genutzt werden kann. Für die Datenverarbeitung innerhalb dieses durch Verschlüsselung geschlossenen Systems sind jedoch einzig die am Projekt beteiligten Parteien Verantwortliche oder Auftragsverarbeiter.

---

23 *Finck*, Blockchain and Data Protection in the European Union, EDPL 1/2018, 17 (26); *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1254).

24 Siehe dazu bereits B.II.2.

b) Verantwortlichkeit von öffentlichen Stellen und Zentralstelle

Die Entscheidung darüber, ob Daten in die Blockchain gespeichert und über einen Verweis bereitgestellt werden, trifft die jeweils einpflegende öffentliche Stelle. Sie verfolgt dabei auch willentlich den Zweck, diese Daten anderen öffentlichen Stellen zur Verfügung zu stellen. Für die Frage der Verantwortlichkeit ist dabei unbeachtlich, ob sie hierzu auch verpflichtet ist. Entscheidet sich die öffentliche Stelle zur Einpflegung der Daten, so ist sie aber bezüglich der Wahl der Mittel eingeschränkt. Durch die Vorgaben des Systems können regelmäßig nur von der Zentralstelle vorgesehene Datensätze übermittelt werden. Die Entscheidung, welche Adressaten eine Leseberechtigung erhalten, wird nicht von der jeweils einspeichernden öffentlichen Stelle, sondern ebenfalls von der Zentralstelle getroffen. Zwar kann die öffentliche Stelle die Daten, welche durch die Verlinkung auf dem eigenen System gespeichert sind, jederzeit löschen. Eine Löschung der Daten in der Blockchain ist der öffentlichen Stelle hingegen nicht möglich.

Es lässt sich damit zumindest festhalten, dass nach der bisherigen Konzeption des Projekts die einpflegende öffentliche Stelle nicht alleine über die Zwecke und Mittel der Datenverarbeitung entscheiden kann. Folglich ist sie auch nicht allein Verantwortliche. Weiter lässt sich festhalten, dass die Zentralstelle, diejenige ist, die das System implementiert, die Vorgaben für die einzuspeichernden Daten stellt und durch die Programmierung der Rechte- und Rollen darüber entscheidet, wer Lesezugriff auf die gespeicherten Daten erhält. Somit ist diese zumindest Mitverantwortliche für die Datenverarbeitung.[25]

Dies eröffnet zunächst zwei Gestaltungsmöglichkeiten: einerseits könnte die Zentralstelle als alleinige Verantwortliche sich für die Einpflegung der Daten der öffentlichen Stellen als Auftragsverarbeiter bedienen, andererseits ist denkbar, dass sich die öffentlichen Stellen und die Zentralstelle die Verantwortlichkeit für die Einpflegung der Daten teilen. Eine alleinige

---

25 Ebenso *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1255); *Bitkom*, Faktenpapier: Blockchain und Datenschutz, S. 30, abrufbar unter: https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html (zuletzt abgerufen am: 15.06.2018).

Verantwortlichkeit der einpflegenden öffentlichen Stelle erscheint hingegen nur bei Änderungen der bisherigen Konzeption möglich.[26]

(1) Die öffentlichen Stellen als Auftragsverarbeiter nach Art. 28 DSVGO

Denkbar ist eine Konstellation, in der die Verantwortlichkeit für die Datenverarbeitung allein von der Zentralstelle übernommen wird und die öffentlichen Stellen als Auftragsverarbeiter der Zentralstelle tätig werden. Voraussetzung ist eine Auftragsverarbeitungsvereinbarung zwischen den öffentlichen Stellen und der Zentralstelle nach Art. 28 Abs. 3 DS-GVO. Die öffentlichen Stellen würden bei der Datenverarbeitung alleine nach Weisung der Zentralstelle handeln, welche die Pflichten des Verantwortlichen alleine übernähme. Die Zentralstelle hätte dafür Sorge zu tragen, dass die Datenverarbeitung durch die öffentlichen Stellen datenschutzrechtskonform durchgeführt wird und wäre gegenüber den betroffenen Migranten betreffend etwaiger Ansprüche alleiniger Anspruchsgegner.

Zweifel begegnen einer solchen Gestaltung vor dem Hintergrund, dass die Verfügungshoheit über den Großteil der Daten bei der jeweils einpflegenden öffentlichen Stelle verbleibt. Bei der Zentralstelle liegen, anders als beim Ausländerzentralregister, keine Kopien der Daten vor. Eine Gestaltung mit Auftragsverarbeitung erfordert, dass die von der öffentlichen Stelle bereitgestellten Daten nur für die Zwecke der Übermittlung gesondert gespeichert werden und nach Weisung der Zentralstelle verwendet und gelöscht werden. Die teilnehmenden öffentlichen Stellen müssten in diesem Fall ihre Entscheidung über die Verwendung der Daten in die Hände der Zentralstelle legen.

(2) Öffentliche Stellen und Zentralstelle als gemeinsam Verantwortliche nach Art. 26 DS-GVO

Die Rollenverteilung zwischen der initiierenden Zentralstelle und den mitwirkenden öffentlichen Stellen eröffnet auch die Möglichkeit einer gemeinsamen Verantwortlichkeit beider Stellen. Während die öffentlichen Stellen darüber entscheiden, ob und welche Daten weitergegeben werden, wird durch die Zentralstelle die Entscheidung über den Verbreitungsweg und die Leseberechtigung der übrigen öffentlichen Stellen getroffen. Voraussetzung für eine

---

26 Ähnliche Gestaltungsmöglichkeiten sieht auch der *Blockchain Bundesverband*, Blockchain, data protection and the GDPR, v.1.0, 25.05.2018, S.7.

gemeinsame Verantwortlichkeit ist gem. Art. 26 Abs. 1 DS-GVO eine Vereinbarung der Parteien in transparenter Form über die Aufgabenverteilung. Hierbei muss sich auch darüber geeinigt werden, wer welche Verpflichtungen gegenüber dem Betroffenen übernimmt. Das wesentliche dieser Vereinbarung muss den Migranten nach Art. 26 Abs. 2 S. 2 DS-GVO zur Verfügung gestellt werden. Eine Geltendmachung der Rechte des Migranten ist jedoch nach Art. 26 Abs. 3 DS-GVO gegenüber jedem der Verantwortlichen möglich.

Für diese Lösung spricht die Tatsache, dass die Daten tatsächlich nicht an die Zentralstelle abgegeben werden. Den öffentlichen Stellen würde die Möglichkeit eröffnet, die Daten, unabhängig von Weisungen der Zentralstelle, auch für eigene interne Zwecke zu nutzen.

(3) Die öffentlichen Stellen als alleinige Verantwortliche

Die einpflegenden öffentlichen Stellen können nur dann alleinige Verantwortliche sein, wenn sie über Zweck und Mittel der Datenverarbeitung frei entscheiden können. Dies erfordert mindestens, dass die Vergabe der Leseberechtigungen an den eingepflegten Daten im Rechte- und Rollensystem von den einpflegenden öffentlichen Stellen selbst vorgenommen werden können. Auch in diesem Fall wird die Infrastruktur für die Datenübermittlung zentral bereitgestellt, die öffentlichen Stellen hätten jedoch die alleinige Kontrolle über die Verbreitung der Daten. Die Zentralstelle hätte keine Möglichkeit, gegen den Willen der jeweiligen öffentlichen Stelle Datenverarbeitungen vorzunehmen. Daher erschiene es in einem solchen Fall möglich, die einpflegende öffentliche Stelle als alleinige Verantwortliche zu bestimmen.

(4) Zusammenfassung der Gestaltungsmöglichkeiten

Für die Umsetzung des Projekts nach der bisherigen Konzeption sind zwei Gestaltungsmöglichkeiten denkbar. Soll die Frage der Verantwortlichkeit an einer Stelle gebündelt werden, so bietet sich eine Auftragsverarbeitungsvereinbarung zwischen den teilnehmenden öffentlichen Stellen und der Zentralstelle an. Die öffentlichen Stellen würden hierdurch von den Pflichten der DS-GVO entbunden, wären jedoch der Zentralstelle gegenüber verantwortlich.

Sollen die öffentlichen Stellen für die Datenweitergabe eine Mitverantwortung tragen, so ist die Vereinbarung einer geteilten Verantwortlichkeit vorzuziehen. Eine Weisungsgebundenheit der öffentlichen Stellen gegenüber der Zentralstelle bezüglich der Datenweitergabe be-

stünde dann nicht. Die Informationspflichten der Art. 13, 14 DS-GVO können in diesem Fall von den beteiligten öffentlichen Stellen gegenüber den Migranten erfüllt werden.

Soll die jeweils einpflegende öffentliche Stelle die alleinige Verantwortlichkeit übernehmen, so muss die Verfügung über die Vergabe der Berechtigungen des Rechte- und Rollensystems in die Hände der einpflegenden Behörde gelegt werden. Eine Datenverarbeitung ohne Kontrolle der einpflegenden Behörde darf nicht möglich sein.

IV. Zwischenfazit

Sowohl bei der Einpflegung und Übermittlung als auch beim Auslesen der Daten kommt es zur Verarbeitung personenbezogener Daten. Hiervon sind sowohl die Off-Chain- als auch die On-Chain-Daten betroffen. Die Verantwortlichkeit für die Einpflegung und Übermittlung der Daten kann entweder eine Zentralstelle alleine oder die einpflegende öffentliche Stelle gemeinsam mit der Zentralstelle übernehmen. Soll die einpflegende öffentliche Stelle die alleine Verantwortliche sein, so muss die Vergabe der Berechtigungen im Rechte- und Rollensystem allein in ihre Hände gelegt werden.

C. Rechtfertigung der Datenverarbeitung

Für die Verarbeitung personenbezogener Daten gilt nach der DS-GVO ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Erlaubnistatbestände finden sich abschließend aufgezählt in Art. 6 Abs. 1 DS-GVO. Vorrangig soll die für die geplante Datenverarbeitung naheliegende Rechtsgrundlage des Art. 6 Abs. 1 lit. e DS-GVO geprüft werden. Übrige Rechtsgrundlagen werden im Anschluss angesprochen.

I. Aufgaben im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

Nach Art. 6 Abs. 1 lit. e DS-GVO ist eine Datenverarbeitung dann gerechtfertigt, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem Verantwortlichen übertragen wurde.

Der Begriff des öffentlichen Interesses ist weit gefasst. Man wird darunter aber zumindest die Ziele der Europäischen Union im Primärrecht anerkennen können.[27] Hierzu gehört nach Art. 3 Abs. 2 EUV u.a. das Recht auf Asyl. Die Gewährung des Rechts auf Asyl erfordert ein geordnetes Asylverfahren. Dessen Durchführung und die hierfür erforderlichen Datenübermittlungen liegen folglich im öffentlichen Interesse. Die öffentlichen Stellen handeln bei der Weitergabe der Daten auch in Ausübung öffentlicher Gewalt.

Art. 6 Abs. 1 lit. e DS-GVO kann als Erlaubnisnorm nicht alleine stehen, sondern erfordert nach Art. 6 Abs. 3 DS-GVO für die Verarbeitung eine zusätzliche Rechtsgrundlage im Unionsrecht oder dem Recht der Mitgliedsstaaten, dem der Verantwortliche unterliegt. Es ist für den hier untersuchten Fall davon auszugehen, dass die öffentlichen Stellen dem Recht der Bundesrepublik Deutschland unterliegen. Als nationale Rechtsgrundlage kommt daher zunächst das für das Ausländerzentralregister geschaffene Ausländerzentralregistergesetz (AZRG) in Betracht. Daneben sind die allgemeinen Datenschutzgesetze relevant. Abhängig davon, ob sich die Handlung der jeweils tätig werdenden öffentlichen Stelle nach dem Bundesrecht oder dem Landesrecht richtet, muss das jeweils einschlägige Datenschutzgesetz Anwendung finden. Hier soll exemplarisch das neue Bundesdatenschutzgesetz (BDSG neu) herangezogen werden.

---

27 Sydow/*Reimer*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 6, Rn. 40.

1. Datenübermittlung nach dem AZRG

Im AZRG finden sich zahlreiche Rechtsgrundlagen für die Übermittlung personenbezogener Daten über Migranten. Die §§ 6 ff. AZRG regeln die Übermittlung der Daten an die Registerbehörde, die §§ 10 ff. AZRG die Übermittlung von der Registerbehörde an öffentliche Stellen. § 22 AZRG erlaubt dafür unter bestimmten Voraussetzungen auch einen Abruf der Daten im automatisierten Verfahren. Die §§ 25 ff. AZRG normieren schließlich die Datenweitergabe von der Registerbehörde an nichtöffentliche Stellen, Behörden anderer Staaten und über- und zwischenstaatliche Stellen.

Für eine Anwendbarkeit der Vorschriften des AZRG könnte sprechen, dass das BAMF durch die von ihr koordinierte Vernetzung der lokalen Speicher der öffentlichen Stellen ein dem Ausländerzentralregister vergleichbares Register schafft. Durch die Festlegung der Lesebefugnisse kann das BAMF darüber entscheiden, welchen Stellen ein automatisierter Abruf gem. § 22 AZRG erlaubt ist. Sieht man das BAMF, als Zentralstelle, als den für die Übermittlung der Daten Verantwortlichen an,[28] so könnte dies für eine Anwendbarkeit der Normen des AZRG sprechen.

Einer solchen Lösung begegnen jedoch gewichtige Zweifel. Der Unterschied zwischen dem Ausländerzentralregister und der geplanten Mobilisierung von Daten zwischen den öffentlichen Stellen mittels einer Permissioned-Blockchain liegt darin, dass die Daten nicht bei der Registerbehörde zentral zwischengespeichert werden, sondern über die Blockchain ein direkter Austausch der Daten zwischen den öffentlichen Stellen stattfindet. Das AZRG ist allein für den konkreten Fall des Ausländerzentralregisters zugeschnitten. § 1 Abs. 2 AZRG normiert, dass die Speicherung und Übermittlung der Daten durch die Registerbehörde selbst vorgenommen wird. Anhand der im AZRG vorgenommenen Differenzierung zwischen den Regelungen für die Übermittlung an die Registerbehörde und den Regelungen für die Übermittlung von der Registerbehörde an Dritte wird deutlich, dass das Gesetz nur den Fall eines zentral geführten Registers unter der Verfügungsmacht der Registerbehörde erfassen will. Eine extensive Auslegung der Vorschriften, welche auch die Führung eines Zentralregisters durch eine dezentrale Blockchain-Lösung umfasst, ist mit dem Wortlaut und der Systematik des AZRG nicht vereinbar. Einer analogen Anwendung steht entgegen, dass durch Einführung

---

28 Siehe hierzu bereits B.III.2.a).

des § 25 BDSG neu keine Regelungslücke besteht. Im Ergebnis sind die Normen des AZRG daher keine taugliche Rechtsgrundlage für die Datenübermittlung im geplanten Blockchain-Vorhaben.

2. Datenübermittlung zwischen öffentlichen Stellen nach dem BDSG neu

Stattdessen könnte die Datenverarbeitung nach den Normen des BDSG neu gerechtfertigt sein. § 3 BDSG neu wiederholt zunächst lediglich den Wortlaut des Art. 6 Abs. 1 lit. e DS-GVO. Demnach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Für den speziellen Fall der Datenübermittlung durch öffentliche Stellen an öffentliche Stellen normiert § 25 Abs. 1 BDSG neu die Zulässigkeit der Übermittlung für den Fall, dass die Daten zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist.

Als zusätzliche Voraussetzung nennt die Norm die Einschlägigkeit einer der sechs Fälle des § 23 Abs. 1 BDSG neu. Diese betreffen eigentlich diejenigen Konstellationen, bei denen die Datenverarbeitung zu einem anderen als dem ursprünglichen Zweck der Datenerhebung erfolgt. Erfolgt die Datenerhebung bereits ursprünglich (auch) mit dem Zweck der späteren Weitergabe an andere öffentliche Stellen, so ist hingegen nicht einleuchtend, warum die zusätzlichen Voraussetzungen des § 23 Abs. 1 BDSG neu gelten sollen.[29] Auch im vorliegenden Fall werden die Daten bei den Migranten von den öffentlichen Stellen auch mit dem Zweck erhoben, diese im Laufe des Verfahrens an andere öffentliche Stellen weiterzugeben. Es ist daher davon auszugehen, dass die Voraussetzungen des § 25 Abs. 1 BDSG neu für eine Datenübermittlung genügen. Letztlich bleibt es daher bei der Ausgangsfrage, ob die konkrete Datenübermittlung zur Erfüllung der Aufgaben der übermittelnden oder empfangenden öffentlichen Stellen erforderlich ist.

---

29 So auch Kühling/Buchner/*Herbst*, BDSG, 2. Aufl. 2018, § 25, Rn. 6.

3. Erforderlichkeitsmaßstab

Der Begriff der Erforderlichkeit ist als solcher des Unionsrechts ein eigenständiger Begriff des Gemeinschaftsrechts und in allen Mitgliedsstaaten einheitlich auszulegen.[30] Demnach ist eine Datenverarbeitung dann erforderlich, wenn der Verzicht auf die konkrete Datenverarbeitung zur Unmöglichkeit der Aufgabenerfüllung der öffentlichen Stelle führt.

Ohne die erforderlichen Informationen sind die öffentlichen Stellen grundsätzlich nicht in der Lage ihre Aufgaben zu erfüllen. Die Weitergabe der Informationen könnte hingegen auf direktem Wege zwischen den öffentlichen Stellen stattfinden. Durch die Speicherung in der Blockchain kommt es zu zusätzlichen Datenverarbeitungen, die nicht zwingend erforderlich sind. Der EuGH hat jedoch für den Fall des Ausländerzentralregisters betont, dass eine zentrale Speicherung von Daten auch dann als erforderlich gelten kann, wenn hierdurch eine effizientere Anwendung aufenthaltsrechtlicher Vorschriften ermöglicht wird.[31] Hieraus lässt sich für den Einsatz einer Blockchain-Lösung schließen, dass auch diese dem Erforderlichkeitsmaßstab genügen kann, wenn sie zu einer effizienten Datenübermittlung zwischen den öffentlichen Stellen führt. Eine direkte Übermittlung der Daten zwischen den öffentlichen Stellen ist nicht praktikabel. Durch den Verzicht auf eine Kopie der Daten in einem Zentralregister, ist die Datenverarbeitung im Vergleich zum AZR sogar eingeschränkt. Kopien der Verweise auf der Blockchain liegen nur in sicher verschlüsselter Form vor. Es ist daher davon auszugehen, dass die Datenübermittlung über die Blockchain die Effizienz steigern kann.

Voraussetzung bleibt jedoch auch hier, dass die jeweils empfangende öffentliche Stelle die konkret übermittelten Daten zur Erfüllung ihrer Aufgaben zwingend benötigt. Für die Frage der Erforderlichkeit im Einzelfall können die Normen des AZRG als Richtwert dienen. Zwar sind diese aufgrund ihres Zuschnitts auf den Fall des Ausländerzentralregisters nicht direkt anwendbar, den Normen liegen jedoch Überlegungen darüber zugrunde, welchen öffentlichen Stellen zu welchen Zwecken Zugriff auf die Daten der Migranten gewährt werden sollen. Durch eine entsprechende Programmierung muss sichergestellt werden, dass nur diejenigen öffentlichen Stellen Lesezugriff auf die gespeicherten Daten erhalten, denen nach dem

---

30 *EuGH*, Urteil vom 16.12.2008, Rs. C-524/06, Rn. 52; Kühling/Buchner/*Buchner/Petri*, BDSG, 2. Aufl. 2018, § 6, Rn. 118.

31 *EuGH*, Urteil vom 16.12.2008, Rs. C-524/06, Rn. 66.

AZRG die entsprechenden Daten übermittelt hätten werden dürfen. Dies muss durch eine entsprechende Programmierung der Leseberechtigungen im Rechte- und Rollen-System umgesetzt werden.

II. Sonstige Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO

1. Einwilligung des Betroffenen

Eine Datenverarbeitung ist nach Art. 6 Abs. 1 lit. a DS-GVO rechtmäßig, wenn die betroffene Person hierfür ihre Einwilligung für einen oder mehrere bestimmte Zwecke erteilt. Es erscheint grundsätzlich denkbar, dass von den Migranten die Einwilligung zur Datenweitergabe für den Zweck des Datenaustausches zwischen den öffentlichen Stellen erteilt wird. Eine solche Einwilligung muss jedoch nach Art. 7 Abs. 1 DS-GVO vom Verantwortlichen nachgewiesen werden. Zudem ist diese nach Art. 7 Abs. 3 DS-GVO jederzeit widerruflich. Aus diesem Grund ist zumindest das alleinige Abstellen auf eine erteilte Einwilligung durch den Migranten nicht ratsam.

2. Rechtliche Verpflichtung des Verantwortlichen

Die Datenverarbeitung ist nach Art. 6 Abs. 1 lit. c DS-GVO rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Die öffentlichen Stellen können rechtlich dazu verpflichtet werden, die Daten untereinander auszutauschen. Geht es dabei jedoch um die Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen, so ist Art. 6 Abs. 1 lit. e DS-GVO die speziellere Erlaubnisnorm.

3. Lebenswichtige Interessen des Betroffenen

Eine Datenverarbeitung ist nach Art. 6 Abs. 1 lit. d DS-GVO auch dann gerechtfertigt, wenn lebenswichtige Interessen der betroffenen Person diese erforderlich machen. Hierfür müsste der Datenaustausch zwischen den öffentlichen Stellen im Rahmen des Asylverfahrens dem Schutz lebenswichtiger Interessen der betroffenen Migranten dienen. Als Beispiele für lebenswichtige Interessen nennt Erwägungsgrund 112 S. 2 DS-GVO die körperliche Unversehrtheit und das Leben. Eine unmittelbare Gefahr für Leib und Leben der Migranten droht jedoch bei Ausbleiben der Datenweitergabe nicht. Erwägungsgrund 46 S. 2 DS-GVO macht zudem deutlich, dass auf den Erlaubnistatbestand nur dann abzustellen ist, wenn eine ande-

re Rechtsgrundlage nicht in Betracht kommt. Folglich können lebenswichtige Interessen des Betroffenen nicht zur Rechtfertigung herangezogen werden.

4. Berechtigtes Interesse des Verantwortlichen oder eines Dritten

Eine Berufung auf ein berechtigtes Interesse des Verantwortlichen oder eines Dritten ist gem. Art. 6 Abs. 1 lit. f S. 2 DS-GVO für das Handeln der Behörden in Erfüllung ihrer Aufgaben nicht möglich. Die Datenübermittlung erfolgt hier in Erfüllung der Aufgaben der am Verfahren beteiligten öffentlichen Stellen. Folglich besteht keine Möglichkeit für eine Rechtfertigung aufgrund eines berechtigten Interesses.

D. Umgang mit sensiblen Daten nach Art. 9 DS-GVO

Art. 9 DS-GVO normiert für einen Katalog sensibler personenbezogener Daten spezielle Rechtfertigungsgründe. In Art. 9 Abs. 1 DS-GVO findet sich das grundsätzliche Verbot der Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie der Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Diese Daten sind ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel und verdienen daher einen besonderen Schutz.[32] Eine Verarbeitung dieser Daten ist nur in den abschließend aufgezählten Fällen des Art. 9 Abs. 2 DS-GVO gestattet. Dies bedeutet nicht, dass eine Verarbeitung in diesen Fällen immer gerechtfertigt ist. Vielmehr muss zudem ein Rechtfertigungstatbestand nach Art. 6 DS-GVO einschlägig sein.

Für die folgende Betrachtung ist davon auszugehen, dass über die Blockchain und die Verlinkung auf lokale Datenbestände nur solche Daten übermittelt werden, die nach § 3 AZRG bislang im Ausländerzentralregister gespeichert werden. Im Folgenden sollen zunächst die relevanten Daten ermittelt und sodann das Vorliegen eines Ausnahmetatbestandes nach Art. 9 Abs. 2 DS-GVO geprüft werden.

I. Relevante Daten nach § 3 AZRG

Für die nach § 3 AZRG zu verarbeitenden Daten sind vor allem die Verbote der Verarbeitung von Daten über die rassische und ethnische Herkunft, politische Meinungen und religiöse und weltanschauliche Überzeugungen relevant. Zudem ist eine Verarbeitung von biometrischen Daten und Gesundheitsdaten denkbar.

1. Angaben über die rassische und ethnische Herkunft

Mit dem grundsätzlichen Verbot der Verarbeitung von Daten, die Angaben zur rassischen Herkunft eines Menschen machen, soll einer Kategorisierung von Menschen in Rassen und

---

32 DS-GVO, Erwägungsgrund 51 S. 1.

einer Abwertung von Personengruppen entgegengewirkt werden.[33] Es geht dabei um Eigenschaften der Person, die tatsächlich oder vermeintlich vererbbar sind.[34]

Demgegenüber ist unter der ethnischen Herkunft die Zuordnung zu einer Menschengruppe mit einheitlicher Kultur zu verstehen. Charakteristisch hierfür kann eine gemeinsame Sprache oder Geschichte sein.[35]

a) Staatsangehörigkeit, § 3 Abs. 1 Nr. 4 AZRG

Zu den Grundpersonalien, die nach § 3 Abs. 1 Nr. 4 AZRG im Ausländerzentralregister gespeichert werden, gehört die Staatsangehörigkeit. Alleine aus dieser lassen sich jedoch keine vererbbaren Eigenschaften des Migranten ableiten. Eine Information über die rassische Herkunft enthält die Staatsangehörigkeit daher nicht. Sie wird einer Person nach den jeweiligen Normen des entsprechenden Staates bei Vorliegen der Voraussetzungen verliehen. Die Angehörigkeit einer Menschengruppe mit einheitlicher Kultur oder das Sprechen einer bestimmten Sprache lassen sich hieraus hingegen regelmäßig nicht schließen. Folglich enthält die Staatsangehörigkeit auch keine Informationen über die ethnische Herkunft des Menschen.[36]

b) Status des Asylberechtigten

Auch der Status als Asylberechtigter deutet nicht auf vererbbare Eigenschaften oder die Angehörigkeit zu einer Menschengruppe mit einheitlicher Kultur hin.[37]

2. Religiöse und weltanschauliche Überzeugungen

Vor dem Hintergrund des Diskriminierungsverbots (Art. 21 GRCh), des Gebots der religiösen Vielfalt (Art. 22 GRCh) und des Schutzes der Glaubens- und Gewissensfreiheit (Art. 10 GRCh) sind Angaben, aus denen sich die religiöse und weltanschauliche Überzeugung ergeben,

---

33 Ehmann/Selmayr/*Schiff*, EU-DS-GVO, 1. Aufl. 2017, Art. 9, Rn. 11.
34 Dreier/*Heun*, GG, Art. 3, Rn. 128.
35 Ehmann/Selmayr/*Schiff*, EU-DS-GVO, 1. Aufl. 2017, Art. 9, Rn. 13.
36 So auch Sydow/*Kampert*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9, Rn. 7; Taeger/Gabel/*Buchner*, BDSG, § 3, Rn. 59.
37 Plath/*Schreiber*, BDSG, § 3, Rn. 79.

grundsätzlich verboten.[38] Religiöse Überzeugungen gehen in erster Linie auf die Lehren der großen Weltreligionen zurück, erfasst sein können aber auch Naturreligionen oder Sekten.[39]

a) Namen, Geburtsort und –bezirk, § 3 Abs. 1 Nr. 4 AZRG

Nach § 3 Abs. 1 Nr. 4 AZRG gehören zu den zu speichernden Grundpersonalien der Familienname, Geburtsname, Vornamen, der Geburtsort und –bezirk. Teilweise wird angenommen, dass sich aus diesen Angaben bereits Rückschlüsse auf eine Religionszugehörigkeit ziehen lassen, wenn beispielsweise ein typischer Familienname in einer stark von einer bestimmten Glaubensrichtung geprägten Region vorkommt.[40] Eine gewisse Wahrscheinlichkeit genügt jedoch für den Rückschluss auf die Zugehörigkeit zu einer Religionsgemeinschaft nicht. Anders als der Familienname, der Geburtsort und –bezirk können religiöse Überzeugungen vom Betroffenen frei gewählt werden.[41] Demnach wird man davon ausgehen müssen, dass die Angaben zu den Grundpersonalien keine Informationen über die religiöse Überzeugung des Migranten enthalten.

b) Die Religionszugehörigkeit, § 3 Abs. 1 Nr. 5 AZRG

Art. 9 Abs. 1 DS-GVO ist hingegen für die Religionszugehörigkeit einschlägig, die nach § 3 Abs. 1 Nr. 5 AZRG, bei Vorliegen einer Einwilligung des Migranten, gespeichert wird.

3. Biometrische Daten

Der Begriff der biometrischen Daten ist in Art. 4 Nr. 14 DS-GVO legal definiert als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten".

a) Fingerabdrücke, § 3 Abs. 2 Nr. 1 AZRG

Für Ausländer, die ein Asylgesuch geäußert haben, unerlaubt eingereist sind oder sich unerlaubt im Geltungsbereich des AZRG aufhalten, sowie für Ausländer, die einen Asylantrag ge-

---

38 Kühling/Buchner/*Weichert*, DS-GVO, 2. Aufl. 2018, Art. 9, Rn. 28.
39 Sydow/*Kampert*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9, Rn. 9.
40 Paal/Pauly/*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 9, Rn. 13.
41 So auch Kühling/Buchner/*Weichert*, DS-GVO, 2. Aufl. 2018, Art. 9, Rn. 29.

stellt haben oder über deren Übernahme nach den Rechtsvorschriften der Europäischen Gemeinschaft oder eines völkerrechtlichen Vertrages zur Durchführung eines Asylverfahrens entschieden ist, werden nach § 3 Abs. 2 Nr. 1 AZRG zusätzlich Fingerabdruckdaten und die dazugehörigen Referenznummern gespeichert. Diese sind daktyloskopische Daten i.S.d. Art. 4 Nr. 14 DS-GVO.

b) Größe und Augenfarbe, § 3 Abs. 2 Nr. 2 AZRG

Unter denselben Voraussetzungen werden nach § 3 Abs. 2 Nr. 2 AZRG auch Größe und Augenfarbe des Migranten gespeichert. Diese Daten enthalten Informationen zu den physischen Eigenschaften der Person. Größe und Augenfarbe erlauben jedoch keine eindeutige Identifikation einer Person, da sie auch in der Kombination bei einer Vielzahl von Menschen in gleicher Weise auftreten können. Folglich handelt es sich bei diesen nicht um biometrische Daten nach Art. 9 Abs. 1 DS-GVO.

4. Gesundheitsdaten

In Art. 4 Nr. 15 DS-GVO wird der Begriff der Gesundheitsdaten legaldefiniert als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen." Dabei ist der gegenwärtige, frühere und künftige Gesundheitszustand erfasst.[42]

a) Durchführung einer Gesundheitsuntersuchung, § 3 Abs. 2 Nr. 10 AZRG

Für Ausländer, die ein Asylgesuch geäußert haben, unerlaubt eingereist sind oder sich unerlaubt im Geltungsbereich des AZRG aufhalten, sowie für Ausländer, die einen Asylantrag gestellt haben oder über deren Übernahme nach den Rechtsvorschriften der Europäischen Gemeinschaft oder eines völkerrechtlichen Vertrages zur Durchführung eines Asylverfahrens entschieden ist, werden nach § 3 Abs. 2 Nr. 10 AZRG i.V.m. § 62 Abs. 1 AsylG und § 36 Abs. 4 und 5 IfSG Daten über die Durchführung einer Gesundheitsuntersuchung auf übertragbare Krankheiten und das Vorliegen einer ansteckenden Lungentuberkulose gespeichert. Aus die-

42 DS-GVO, Erwägungsgrund 35 S. 1.

sen Daten gehen Informationen über den Gesundheitszustand des Migranten hervor. Folglich handelt es sich um Gesundheitsdaten nach Art. 9 Abs. 1 DS-GVO.

b) Feststellung der medizinischen Unbedenklichkeit einer Unterbringung, § 3 Abs. 2 Nr. 10a AZRG

Unter denselben Voraussetzungen wie für Speicherung von Daten über Gesundheitsuntersuchungen werden nach § 3 Abs. 2 Nr. 10a AZRG Daten über die Feststellung, dass keine medizinischen Bedenken gegen die Aufnahme in eine Einrichtung der gemeinschaftlichen Unterbringung bestehen, gespeichert. Zwar enthalten diese Daten keine Hinweise auf konkrete Krankheiten, es gehen jedoch Informationen über den Gesundheitszustand des Migranten aus ihr hervor. Auch bei diesen handelt es sich daher um Gesundheitsdaten nach Art. 9 Abs. 1 DS-GVO.

c) Impfungen, § 3 Abs. 2 Nr. 11 AZRG

Unter denselben Voraussetzungen werden nach § 3 Abs. 2 Nr. 11 AZRG Daten über die Durchführung von Impfungen gespeichert. Durch diese Daten lassen sich Informationen über den gegenwärtigen und zukünftigen Gesundheitszustand des Migranten gewinnen. Auch diese sind daher Gesundheitsdaten nach Art. 9 Abs. 1 DS-GVO.

5. Zwischenergebnis

Das AZRG sieht vereinzelt Datenverarbeitungen vor, die unter das grundsätzliche Verbot des Art. 9 Abs. 1 DS-GVO fallen. Hierzu zählen die Angaben zur Religionszugehörigkeit, Fingerabdrücke und Angaben zu Gesundheitsuntersuchungen und gesundheitlichen Maßnahmen.

II. Ausnahmen nach Art. 9 Abs. 2 DS-GVO

Nach Art. 9 Abs. 2 DS-GVO gilt das Verbot der Verarbeitung nicht in den dort abschließend aufgezählten Fällen. Für die vorliegende Betrachtung ist - neben der ausdrücklichen Einwilligung - möglicherweise eine Verarbeitung zu Archivzwecken im öffentlichen Interesse, für wissenschaftliche oder historische Forschungszwecke, für statistische Zwecke oder aus Gründen eines erheblichen öffentlichen Interesses relevant.

1. Ausdrückliche Einwilligung

Eine Verarbeitung ist nach Art. 9 Abs. 2 lit. a DS-GVO mit ausdrücklicher Einwilligung der betroffenen Person für einen oder mehrere festgelegte Zwecke möglich. Eine Beschränkung auf bestimmte Verarbeitungszwecke findet nicht statt. Im Gegensatz zu Art. 6 Abs. 1 lit. a, 7 DS-GVO muss die Einwilligung ausdrücklich erfolgen. Konkludente Einwilligungen sind hierdurch ausgeschlossen. Zwar kann eine ausdrückliche Einwilligung auch mündlich erfolgen, zu Beweiszwecken sollte jedoch eine schriftliche Fixierung vorgenommen werden.[43] Entscheidend ist weiter, dass die Einwilligung unmittelbaren Bezug auf die Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten Daten nimmt und der Verwendungszusammenhang offen gelegt wird.[44] Dem Betroffenen muss also deutlich gemacht werden, für welche Zwecke die Daten verarbeitet werden.

Nach § 3 Abs. 1 Nr. 5 AZRG sind die Angaben zur Religionszugehörigkeit nur dann zu speichern, wenn sie freiwillig abgegeben wurden. Art. 9 Abs. 2 lit. a DS-GVO geht darüber hinaus. Dem Migranten muss bei der Abgabe der Einwilligung auch der Zweck der Datenverarbeitung offen gelegt werden, sodass er eine informierte Entscheidung über die Speicherung der Daten treffen kann.

Die Einholung einer Einwilligung ist zwar möglich, in der Praxis jedoch aus den bereits genannten Gründen[45] wenig praktikabel. Das Erfordernis der Ausdrücklichkeit erschwert die Einholung zusätzlich.

2. Archivzwecke, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke

Nach Art. 9 Abs. 2 lit. j DS-GVO ist die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO möglich, solange es hierfür eine Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaates gibt. Eine solche findet sich auf Bundesebene in den §§ 27, 28 BDSG neu. Zudem erlaubt § 24a AZRG die Verarbeitung und Nutzung personenbezogener Daten für wissenschaftliche Zwecke. Die Normen sind jedoch nur dann an-

---

43 So auch Sydow/*Kampert*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 9, Rn. 14.
44 Kühling/Buchner/*Weichert*, DS-GVO, 2. Aufl. 2018, Art. 9, Rn. 47.
45 Siehe hierzu bereits C.II.1.

wendbar, wenn es sich bei der geplanten Datenverarbeitung im Rahmen des Blockchain-Vorhabens um einen der in Art. 9 Abs. 2 lit. j DS-GVO genannten Zwecke handelt.

a) Archivzwecke im öffentlichen Interesse

Eine Verarbeitung zu Archivzwecken, dient der Aufzeichnung von Daten von bleibendem Wert für das allgemeine öffentliche Interesse.[46] Die Privilegierung lässt sich auf den Schutz der Informationsfreiheit nach Art. 11 GRCh zurückführen.[47] Vor diesem Hintergrund geht es um die Sicherstellung kultureller Überlieferungszusammenhänge[48] und die Bewahrung der Genesis politischer und gesellschaftlicher Ergebnisse[49].

Die Aufzeichnungen im Rahmen des Blockchain-Verfahrens ließen sich lediglich als Dokumentation des politischen Ereignisses der Flüchtlingskrise werten. Jedoch steht einer Einordnung als Archiv die mangelnde öffentliche Zugänglichkeit entgegen. Die Datenübermittlung dient alleine der Abwicklung interner Verwaltungsvorgänge. Eine Bereicherung der Öffentlichkeit mit Informationen ist nicht Zweck des Vorhabens. Folglich wird man davon ausgehen müssen, dass die Datenverarbeitung nicht Archivzwecken im öffentlichen Interesse dient.

b) Wissenschaftliche oder historische Forschungszwecke

Relevanz können für den vorliegenden Fall nur wissenschaftliche Forschungszwecke haben. Historische Forschungszwecke sollen bei der Betrachtung daher außen vor bleiben. Erwägungsgrund 159 fordert eine weite Auslegung des Begriffs der wissenschaftlichen Forschung. Hintergrund der Privilegierung ist die in Art. 13 GRCh festgeschriebene Wissenschaftsfreiheit[50] und das in Artikel 179 AEUV genannte Ziel, einen europäischen Raum der Forschung

---

46 DS-GVO, Erwägungsgrund 158 S. 2.
47 Paal/Pauly/*Pauly*, DS-GVO, 2. Aufl. 2018, Art. 89, Rn. 6.
48 Sydow/*Hense*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 89, Rn. 7.
49 Kühling/Buchner/*Buchner/Tinnefeld*, DS-GVO, 2. Aufl. 2018, Art. 89, Rn. 10.
50 So auch Kühling/Buchner/*Buchner/Tinnefeld*, DS-GVO, 2. Aufl. 2018, Art. 89, Rn. 13.

zu schaffen[51]. Zum Schutzbereich der Wissenschaftsfreiheit zählt jeder nach Inhalt und Form ernsthafte und planmäßige Versuch zur Ermittlung der Wahrheit.[52]

Vor dem Hintergrund der Wissenschaftsfreiheit wäre für die Verarbeitung zu wissenschaftlichen Forschungszwecken zu fordern, dass die Ergebnisse der Datenverarbeitung zur Ermittlung der Wahrheit der Allgemeinheit erkenntnisbringend zur Verfügung gestellt werden sollen. Dies ist im vorliegenden Projekt hingegen nicht geplant. Somit dient die Datenverarbeitung auch nicht wissenschaftlichen Forschungszwecken.

c) Statistische Zwecke

Nach Erwägungsgrund 162 sind unter einem „statistischen Zweck" jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen. Einer Statistik liegt der methodische Umgang mit empirischen Daten zugrunde.[53] Die Ergebnisse der Verarbeitung zu statistischen Zwecken sollen keine personenbezogenen, sondern aggregierte Daten sein und nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.[54]

Die Datenverarbeitung dient dem Austausch von Informationen über konkrete natürliche Personen. Ein methodischer Umgang mit empirischen Daten ist nicht Zweck des Vorhabens. Die Daten liegen nicht in aggregierter Form vor und werden für Maßnahmen und Entscheidungen gegenüber einzelnen natürlichen Personen verwendet. Demzufolge dient die geplante Datenverarbeitung auch nicht statistischen Zwecken.

3. Erhebliches öffentliches Interesse

Eine Verarbeitung kann nach Art. 9 Abs. 2 lit. g DS-GVO auch dann gerechtfertigt sein, wenn sie aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Voraussetzung ist, dass hierfür eine Rechtsgrundlage im Unionsrecht oder dem Recht der Mitgliedsstaaten be-

---

51 DS-GVO, Erwägungsgrund 159 S. 3.

52 BVerfG Urt. v. 29.5.1973 – 1 BvR 424/71, 1 BvR 325/72, BVerfGE 35, 79 (113)– Hochschulurteil; BVerfG Beschl. v. 1.3.1978– 1 BvR 333/75, 1 BvR 174/71, 1 BvR 178/71, 1 BvR 191/71, BVerfGE 47, 327(367)– HUG.

53 Roßnagel/*Richter*, EU-DS-GVO, § 4, Rn. 97.

54 DS-GVO, Erwägungsgrund 162 S. 5.

steht, die in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

a) Ermächtigung durch das AZRG

§ 3 AZRG nennt die betroffenen Daten konkret, die Normen des AZRG erlauben auch deren Verarbeitung. Wie oben bereits dargestellt, sind diese jedoch auf den hier vorliegenden Fall nicht anwendbar.

b) Ermächtigung durch § 22 Abs. 1 Nr. 2 lit. a BDSG neu

Eine weitere mögliche Rechtsgrundlage findet sich in § 22 Abs. 1 Nr. 2 lit. a BDSG neu. Demnach ist öffentlichen Stellen die Datenverarbeitung gestattet, wenn sie u.a. aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist und die Interessen der für die Datenverarbeitung Verantwortlichen die Interessen der betroffenen Person überwiegen. Die §§ 22 Abs. 1 Nr. 2 lit b-d BDSG neu nennen Beispiele für das Vorliegen eines erheblichen öffentlichen Interesses, bleiben jedoch sehr unbestimmt. Es ist daher äußerst zweifelhaft, ob die Norm den oben genannten Anforderungen des Art. 9 Abs. 2 lit. j DS-GVO gerecht wird. Auch wenn ein „zwingendes" Interesse gefordert wird, ist der Anwendungsfall dadurch nicht näher bestimmt. Aus Gründen des Rechtsstaatsprinzips ist zu fordern, dass der nationale Gesetzgeber für die infrage stehenden sensiblen Daten eine konkrete Rechtsgrundlage schafft, die eine Abwägung mit den Grundrechten und Interessen des Betroffenen erkennen lässt. Diesen Anforderungen genügt § 22 Abs. 1 Nr. 2 BDSG neu nicht. Aus diesem Grund kann für die Verarbeitung sensibler Daten nicht alleine auf die BDSG-Norm abgestellt werden.[55] Eine Spezialnorm, die die Datenübermittlung sensibler Daten über eine Blockchain erfasst, besteht de lege lata nicht.

---

55 So auch im Ergebnis Kühling/Buchner/*Weichert*, BDSG, 2. Aufl. 2018, § 22, Rn. 21; Schantz/Wolff/*Schantz*, Neues DatenschutzR, Rn. 716; Paal/Pauly/*Frenzel*, BDSG, 2. Aufl. 2018, § 22, Rn. 10.

III. Zwischenfazit

Einzelne Daten, die bislang nach dem AZRG verarbeitet werden, fallen unter das grundsätzliche Verbot des Art. 9 Abs. 1 DS-GVO. Hiervon sind die Religionszugehörigkeit, Fingerabdrücke und Angaben zu Gesundheitsuntersuchungen und gesundheitlichen Maßnahmen erfasst. Für diese Verarbeitungen ließe sich zwar eine ausdrückliche Einwilligung einholen. Dies erscheint jedoch nicht praktikabel. Andere Rechtsgrundlagen für die Datenverarbeitung sind de lege lata nicht ersichtlich. Für die Umsetzung einer Datenübermittlung mittels einer Blockchain-Lösung bedürfte es daher einer eindeutigen gesetzlichen Grundlage des nationalen Rechts oder des Unionsrechts. Das AZRG ist in seiner derzeitigen Fassung hierfür nicht ausreichend, da es die direkte Datenübermittlung zwischen öffentlichen Stellen über eine Blockchain nicht erfasst. Eine geeignete Rechtsgrundlage müsste zwar nicht ausdrücklich die Datenweitergabe durch eine Blockchain, aber zumindest den Fall der direkten Datenübermittlung zum Zwecke des Datenaustausches im Asylverfahren regeln und eine entsprechende Abwägung der öffentlichen Interessen mit den Interessen der Migranten erkennen lassen.

E. Wahrung der Betroffenenrechte

Eine Herausforderung des geplanten Blockchain-Verfahrens ist die Wahrung der in der DS-GVO normierten Betroffenenrechte. Im Folgenden soll zunächst auf die Informationspflichten (Art. 13, 14 DS-GVO) und das Auskunftsrecht (Art. 15 DS-GVO) eingegangen werden. Sodann wird das Recht auf Berichtigung (Art. 16 DS-GVO) und das Recht auf Löschung (Art. 17 DS-GVO) näher untersucht. Schließlich wird auf das Recht des Betroffenen eingegangen, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22 DS-GVO).

I. Informationspflichten und Auskunftsrecht

Art. 13 DS-GVO normiert für den Fall, dass personenbezogene Daten beim Betroffenen erhoben werden, einen Katalog von Informationen, die dem Betroffenen zum Zeitpunkt der Datenerhebung mitgeteilt werden müssen. Findet die Datenerhebung nicht beim Betroffenen statt, so normiert Art. 14 DS-GVO eine entsprechende Informationspflicht innerhalb einer angemessenen Frist, welche in Art. 14 Abs. 3 DS-GVO näher definiert ist.

Hinsichtlich der Informationspflichten ergeben sich durch den Blockchain-Einsatz keine Besonderheiten. Den betroffenen Migranten sind die Informationen über die Verwendung ihrer personenbezogenen Daten im Zeitpunkt der Erhebung mitzuteilen. Im besten Fall wird bereits bei der Erstregistrierung auf die Verwendung der Daten im Blockchain-Verfahren hingewiesen. Ist dies nicht (mehr) möglich, so müssen die betroffenen Migranten vor der Einpflegung ihrer Daten in die Blockchain nach Art. 14 Abs. 3 lit. c DS-GVO durch die einpflegende öffentliche Stelle informiert werden.

Nach Art. 15 DS-GVO hat der Betroffene das Recht, vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob ihn betreffende persönliche Daten verarbeitet werden. Ist dies der Fall, so kann Auskunft über diese Daten verlangt werden. Zudem muss der Verantwortliche dem Betroffenen die in Art. 15 Abs. 1 DS-GVO genannten Informationen übermitteln.

Auch hier ergeben sich durch den geplanten Blockchain-Einsatz keine Besonderheiten. Der Verantwortliche benötigt jedoch Zugang zu den in der Blockchain über den konkreten Migranten gespeicherten Informationen. Diese müssen dem Migranten auf Verlangen ausgehändigt werden können.

II. Recht auf Vervollständigung

Nach Art. 16 S. 2 DS-GVO hat der Betroffene das Recht, von dem Verantwortlichen – unter Berücksichtigung der Zwecke der Bearbeitung - unverzüglich die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Für die Umsetzung muss zwischen den Off-Chain-Daten und den On-Chain-Daten unterschieden werden.

Die einpflegenden öffentlichen Stellen können die personenbezogenen Off-Chain-Daten, welche auf ihren lokalen Systemen gespeichert sind, jederzeit vervollständigen. Sind die einpflegenden öffentlichen Stellen selbst Verantwortliche, so können sie die Vervollständigung selbstständig vornehmen. Ist die Zentralstelle Verantwortliche, so erfolgt die Vervollständigung auf Weisung der Zentralstelle.

Die Vervollständigung von On-Chain-Daten wird dagegen in der Praxis nicht relevant werden, soweit man davon ausgeht, dass die einpflegende öffentliche Stelle stets die Kennnummer, den Status und den Zeitstempel einpflegen muss. In diesem Fall können die Daten zwar falsch, nicht jedoch unvollständig sein.[56]

III. Recht auf Berichtigung und Löschung

Der Betroffene hat nach Art. 16 S. 1 DS-GVO das Recht, dass ihn betreffende unrichtige personenbezogene Daten unverzüglich berichtigt werden. Zudem hat er das Recht, dass die Daten auf seinen Wunsch unverzüglich gelöscht werden, soweit hierfür ein in Art. 17 Abs. 1 DS-GVO aufgezählter Löschungsgrund vorliegt. Demnach kann im hier betrachteten Verfahren eine Löschung verpflichtend sein, wenn die Daten für die Zwecke ihrer Erhebung nicht mehr erforderlich sind, der Betroffene eine von ihm gegebene Einwilligung zur Verarbeitung der Daten widerruft und keine andere Rechtsgrundlage für die Verarbeitung mehr besteht, der Betroffene rechtmäßig von seinem Widerspruchsrecht gegen die Verarbeitung der Daten Gebrauch macht, die Datenverarbeitung unrechtmäßig erfolgte oder die Löschung der Daten zur Erfüllung einer rechtlichen Verpflichtung aus dem Unionsrecht oder dem Recht der Mitgliedstaaten, der der Verantwortliche unterliegt, erforderlich ist.

S6 Dies gilt umso mehr, wenn die On-Chain-Daten weiter reduziert werden. Siehe dazu sogleich unter E.III.

Für die Berichtigung und Löschung von Off-Chain-Daten stellen sich, ebenso wie für die Vervollständigung, keine besonderen Probleme.[57] Es ist darauf zu achten, dass der Verweis auf die Off-Chain-Daten, welcher on-chain gespeichert ist, keine Informationen enthält, die Rückschlüsse auf die betroffene natürliche Person enthält.

Problematisch ist hingegen die Berichtigung und Löschung von On-Chain-Daten. Dies betrifft Fälle, in denen ein falscher Status, eine falsche öffentliche Stelle oder ein falscher Zeitstempel der Kennnummer des betroffenen Migranten zugeordnet wurde oder die Daten nach Art. 17 DS-GVO gelöscht werden müssen. Für die Berichtigung könnten korrigierte Daten zwar in einem neuen Block gespeichert werden, die falschen Daten müssten jedoch, ebenso wie die nicht mehr erforderlichen Daten, gelöscht werden. Eine Löschung der Daten ist hingegen, aufgrund der Unveränderbarkeit der Blockchain, nach der Einpflegung nicht mehr möglich. Es bedarf daher alternativer Lösungsansätze, um der Berichtigungs- und Löschpflicht nachzukommen. Im Folgenden sollen hierfür drei Optionen vorgestellt werden. Es handelt sich dabei um keine abschließende Aufzählung, sondern lediglich um unverbindliche Vorschläge für eine Umsetzung der Berichtigungs- und Löschpflichten von On-Chain-Daten. Eine Evaluierung ihrer technischen Umsetzungsmöglichkeit für das konkrete Projekt steht aus.

1. Redactable Blockchain

Eine Möglichkeit den Lösch- und Berichtigungspflichten von On-Chain-Daten nachzukommen, kann die Verwendung einer weiter entwickelten „Chameleon-Hash-Funktion" in einer „Redactable Blockchain" sein.[58] Die „Chameleon-Hash-Funktion" wird statt der gewöhnlichen Hash-Funktion zur Verknüpfung der einzelnen Blöcke verwendet und beinhaltet eine „Falltür". Mithilfe eines geheimen Schlüssels ist es möglich, für einen veränderten Input denselben Hashwert zu erzeugen. Auf diese Weise kann der Inhalt eines Blocks nachträglich ma-

---

57 Siehe dazu bereits unter E.II.

58 Das Konzept der Redactable Blockchain wurde vorgestellt von *G. Ateniese, B. Magri, D. Venturi and E. Andrade*, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends," *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, Paris, 2017, pp. 111-126. Ebenfalls vorgeschlagen wird es von *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256 f.); *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, Informatik 2017, 1025 (1030); *Bechtolf/Vogt*, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66 (70); *Finck*, Blockchain and Data Protection in the European Union, EDPL 1/2018, 17 (31).

nipuliert werden, die Kette bleibt hingegen intakt. Die Besonderheit der weiter entwickelten Hash-Funktion in einer „Redactable Blockchain" ist, dass Kollisionen der Hash-Funktion auch nach Veröffentlichung des veränderten Blocks nur mit Kenntnis des Schlüssels gefunden werden können. Somit bleibt die Blockchain trotz der Veränderungen für Dritte unangreifbar. Werden Veränderungen vorgenommen, so sind diese dennoch durch die Teilnehmer des Netzwerks nachvollziehbar. Der Besitzer des Schlüssels kann daher keine unbemerkten Änderungen vornehmen. Der Schlüssel kann von einer Zentralstelle unter Verschluss gehalten und bei Bedarf eingesetzt werden. Alternativ ist es möglich, den Schlüssel unter mehreren Instanzen aufzuteilen und eine Veränderung der Blockchain nur durch die Mitwirkung aller Schlüsselinhaber zu ermöglichen.[59]

Die Umsetzung der Lösch- und Berichtigungspflichten durch Nutzung einer Redactable Blockchain ist grundsätzlich möglich, sie bringt jedoch ebenfalls Herausforderungen mit sich. Zunächst erfordert sie, dass eine eigene Blockchain geschaffen wird. Die Implementierung innerhalb einer unveränderbaren Blockchain, wie der Ethereum-Blockchain, ist nicht möglich. Zudem muss der Schlüssel von einer oder mehreren vertrauenswürdigen Zentralstelle(n) unter Verschluss gehalten werden. Löschungen können dann nur von der Zentralstelle vorgenommen werden.

2. Aufhebung der Verknüpfung zwischen Kennnummer und natürlicher Person

Die on-chain gespeicherten Daten sind zunächst nur deshalb personenbezogen, da die für die Verarbeitung Verantwortlichen über die Kennnummer eine Verknüpfung von Status, bearbeitender öffentlicher Stelle und Zeitstempel zu der natürlichen Person (Migrant) herstellen können. Sobald diese Zuordnung der Kennnummer nicht mehr möglich ist, handelt es sich bei den on-chain gespeicherten Daten nicht mehr um personenbezogene Daten. Die Aufhebung der Möglichkeit zur Identifizierung kommt einer Löschung der Daten gleich.

Es wäre zunächst denkbar, die Kennnummer in allen off-chain Datenbeständen zu löschen, wodurch eine Identifizierung der natürlichen Person nicht mehr möglich wäre. Jedoch müssten alle beteiligten öffentlichen Stellen die Löschung durchführen. Weiter erfordert die Lö-

---

59 *G. Ateniese, B. Mogri, D. Venturi ond E. Androde*, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends," *2017 IEEE Europeon Symposium on Security and Privocy (EuroS&P)*, Paris, 2017, 111 (117).

sung, dass die öffentlichen Stellen Zugriff auf alle Datenträger haben, welche die Kennnummer enthalten. Die Umsetzung dieser Alternative kann sich daher in der Praxis äußerst schwierig gestalten.

Eine weitere Lösung könnte die Schaffung von Umrechnungsschlüsseln sein, die von der jeweils einpflegenden öffentlichen Stelle für jeden Eintrag erstellt werden. Mithilfe des Schlüssels wird aus der Kennnummer, welche außerhalb der Blockchain im Asylverfahren verwendet wird (Off-Chain-Kennung), die Kennnummer berechnet, welche in der Blockchain gespeichert wird (On-Chain-Kennung). Der Schlüssel dient gleichermaßen zur Berechnung in umgekehrter Reihenfolge, ermöglicht also die Ermittlung der Off-Chain-Kennung bei Kenntnis der On-Chain-Kennung. Ohne Kenntnis des Umrechnungsschlüssels dürfen diese Berechnungen nicht möglich sein.

Die jeweils einpflegende öffentliche Stelle speichert den Umrechnungsschlüssel lokal zusammen mit den übrigen Informationen über den Migranten auf dem eigenen System ab. Dabei wird für jeden Eintrag in die Blockchain ein eigener Schlüssel erzeugt. Müssen Daten berichtigt oder gelöscht werden, so entfernt die öffentliche Stelle die lokal gespeicherten Daten inklusive des Umrechnungsschlüssels. In der Blockchain verbleiben lediglich Informationen, welche mit der On-Chain-Kennung verknüpft sind. Diese sind jedoch einer natürlichen Person, ohne Kenntnis des Umrechnungsschlüssels, nicht mehr zuzuordnen.[60]

Durch die Generierung von zu löschenden Umrechnungsschlüsseln kann der Berichtigungs- und Löschfrist nachgekommen werden. Eine verbleibende Schwäche der Lösung ist jedoch die Tatsache, dass auch ohne Kenntnis von der Kennnummer des Migranten durch eine Gesamtschau aller Informationen über Statusänderungen, Zeitstempel und bearbeitende öffentliche Stellen theoretisch Rückschlüsse auf die Identität eines Migranten gezogen werden könnten.[61]

---

60 Ein ähnliches Verfahren stellen auch *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256) vor, wobei diese die jeweils neue Generierung eines Schlüssels für jede Transaktion für impraktikabel halten. Auf die hier vorgeschlagene Möglichkeit eines Verweises auf einen off-chain gespeicherten Schlüssel gehen sie dabei jedoch nicht ein. Ebenfalls angesprochen wird die Möglichkeit von *Bitkom*, Faktenpapier: Blockchain und Datenschutz, S. 18.

61 Siehe hierzu bereits unter B.II.4.b). Dieses Risiko erkennen auch *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256).

3. Off-Chain-Speicherung mit Hashwert-Verknüpfung

Eine weitere Umsetzungsmöglichkeit, welche den Schwächen der vorherigen Lösungen begegnet, besteht darin, auf die Einspeicherung personenbezogener Informationen in der Blockchain gänzlich zu verzichten. Im besten Fall werden sowohl die Kennnummer, der Status und die bearbeitende öffentliche Stelle lediglich off-chain im lokalen System der einpflegenden öffentlichen Stelle gespeichert.

Die einpflegende Stelle speichert bei einer Statusänderung alle Daten lokal ab und bildet von diesen einen Hash-Wert. Ebenjenen veröffentlicht sie zusammen mit dem Verweis auf die Daten in der Blockchain. Durch den Hash-Wert wird sichergestellt, dass weder die einpflegende Stelle noch ein Dritter nachträglich Veränderung der Daten vorgenommen hat. Das System, welches die Rechte und Rollen verteilt, muss Zugriff auf alle Verweise haben, um den Inhalt der lokal gespeicherten Daten auslesen zu können und zu entscheiden, welche öffentlichen Stellen Lesezugriff auf die einzelnen Datenbestände erhalten sollen. Müssen einzelne Daten gelöscht werden, so erfolgt dies durch Löschung der Daten im System der jeweiligen öffentlichen Stelle. Durch den in der Blockchain verbleibenden Verweis und den Hash-Wert sind keine Rückschlüsse auf Informationen über natürliche Personen möglich.[62] Auf diese Weise kann dem Erfordernis der Lösch- und Berichtigungspflicht nachgekommen werden.

4. Zwischenfazit

Die Umsetzung der Betroffenenrechte auf Berichtigung und Löschung stellen eine ernsthafte Herausforderung für die Übermittlung von personenbezogenen Daten über die Blockchain dar. Durch die Einspeicherung der Kennnummer in Verbindung mit dem Status, der bearbeitenden öffentlichen Stelle und dem Zeitstempel verbleiben personenbezogene Daten, auch über den Zeitpunkt der Löschung der lokal bei den öffentlichen Stellen gespeicherten Informationen hinaus, in der Blockchain. Diese Daten müssen entweder ihrerseits gelöscht oder es muss ihnen zumindest durch Aufhebung der Identifizierbarkeit die datenschutzrechtliche Relevanz genommen werden.

---

62 Dies erkennt richtigerweise auch der *Blockchain Bundesverband*, Blockchain, data protection and the GDPR, v.1.0, 25.05.2018, S. 4, 8. Angesprochen wird die Möglichkeit ebenfalls von *Bitkom*, Faktenpapier: Blockchain und Datenschutz, S. 18.

Für die Löschung der Daten kommt grundsätzlich eine „Redactable Blockchain" in Betracht. Eine Aufhebung der Identifizierbarkeit der in der Blockchain gespeicherten Daten kann durch Generierung von Umrechnungsschlüsseln oder dem gänzlichen Verzicht auf die Speicherung von personenbezogenen Informationen im Block erreicht werden.

IV. Keine automatisierte Entscheidung im Einzelfall

Nach Art. 22 DS-GVO hat der Betroffene das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihm gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt. Eine automatisierte Entscheidung liegt zumindest dann vor, wenn maschinell verarbeitete Daten unmittelbar zu einer durch Datenverarbeitungsanlagen getroffenen Entscheidung führen. Auf diese Entscheidung darf, wenn auch nur teilweise, die Bewertung einer natürlichen Person keinen Einfluss nehmen.[63]

Relevante Entscheidungen, die für die betroffenen Migranten rechtliche Wirkung entfalten oder zu einer Beeinträchtigung führen, sind behördliche Handlungen und Verfügungen im Asylverfahren. Zur Entscheidungsfindung werden Daten verwendet, welche durch Datenverarbeitungsanlagen von anderen öffentlichen Stellen übermittelt werden. Die Entscheidung wird jedoch nicht unmittelbar durch die Datenverarbeitungsanlage getroffen. Die Datenverarbeitung dient stattdessen lediglich dem Austausch der Informationen, während die Entscheidung selbst von natürlichen Personen in den jeweils tätigen öffentlichen Stellen getroffen wird. Folglich besteht kein Anwendungsfall des Art. 22 DS-GVO.

---

63 Gola/*Schulz*, DS-GVO, 1. Aufl. 2017, Art. 22, Rn. 12.

F. Datenschutzstrategie durch Technik

Art. 25 DS-GVO verpflichtet den Verantwortlichen zur Einhaltung der Datenschutzgrundsätze durch Technikgestaltung („Privacy by Design") und zur Vornahme von datenschutzfreundlichen Voreinstellungen („Privacy by Default"). Es geht dabei insbesondere darum, die Datenschutzgrundsätze des Art. 5 DS-GVO bereits durch entsprechende Gestaltung der verwendeten Technik zu wahren.[64]

I. Abwägungskriterien

1. Stand der Technik

Nach Art. 25 Abs. 1 DS-GVO ist bei der Implementierung von technischen Maßnahmen der jeweilige „Stand der Technik" zu berücksichtigen. Damit ist ein entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, basierend auf Erkenntnissen aus Wissenschaft, Technik und Erfahrung, gemeint.[65] In der Regel wird man daraus schließen, dass die Techniken bereits eine gewisse Erprobung durchlaufen haben müssen, was aber nicht zwingend heißt, dass sie sich auch durchgesetzt haben müssen.[66]

Als neue Leittechnologie konnte sich die Blockchain-Technologie bislang noch nicht durchsetzen. Die für das konkrete Vorhaben planmäßig einzusetzende Ethereum-Blockchain wurde erst im Jahr 2013 entwickelt,[67] wobei sich in der Zwischenzeit bereits ernstzunehmende Risiken offenbarten.[68]

Andererseits existiert, obwohl die Blockchain-Technologie insgesamt noch vergleichsweise jung ist, ihr ältester Vertreter (Bitcoin) bereits seit 2009.[69] Die Technologie wurde seither intensiv erforscht und laufend angepasst. Eine solche Entwicklung ist auch weiter erkenn-

---

64 Ehmann/Selmayr/*Baumgartner*, EU-DS-GVO, 1. Aufl. 2017, Art. 25, Rn. 1.
65 DIN EN 45020:2006, Ziff. 1.4.
66 Sydow/*Mantz*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 25, Rn. 38.
67 Sie dazu das *Ethereum Whitepaper*, https://vitalik.ca/2017-09-15-prehistory.html (zuletzt abgerufen am: 15.06.2018).
68 https://www.heise.de/newsticker/meldung/Nach-dem-DAO-Hack-Ethereum-glueckt-der-harte-Fork-3273618.html (zuletzt abgerufen am: 15.06.2018).
69 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am: 15.06.2018).

bar.[70] In vielen Branchen findet derzeit eine Erprobung des Einsatzes einer Blockchain statt. Nach nahezu zehn Jahren Laufzeit der ältesten Blockchain lässt sich festhalten, dass die Technologie grundsätzlich funktionstüchtig ist. Sie kann daher zum aktuellen Stand der Technik gezählt werden. Die Berücksichtigung des Stands der Technik erfordert jedoch vom Verantwortlichen, insbesondere in der noch jungen Phase der Technologie, Aufmerksamkeit für neue Entwicklungen und mögliche Schwachstellen.

2. Risiken für die Rechte und Freiheiten der betroffenen Personen

Art. 25 Abs. 1 DS-GVO schreibt für die Einrichtung technischer Schutzmaßnahmen eine Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen vor. Dabei sind solche Risiken gemeint, die zu einem physischen, materiellen oder immateriellen Schaden der betroffenen Personen führen können.[71] Die Norm schreibt zudem eine Abwägung mit der Art, dem Umfang, der Umstände und Zwecke der Datenverarbeitung vor. Diese ist von der Risikobewertung nicht gänzlich zu trennen und kann daher gemeinsam vorgenommen werden. Dabei sollte eine objektive Bewertung des Risikos erfolgen, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko mit sich bringt.[72] An dieser Stelle soll keine umfängliche Datenschutz-Folgenabschätzung erfolgen. Anhand einer Aufzählung möglicher Schäden und der Anzahl der betroffenen Personen und verarbeitenden Stellen sollen aber Anhaltspunkte für die Einschätzung des Risikos der geplanten Datenverarbeitung gegeben werden.

a) Betroffene Rechte und Freiheiten der Migranten

Das Risiko bei der Datenverarbeitung liegt in der Offenlegung der personenbezogenen Daten an unbefugte Personen. Die Offenlegung der Informationen kann den Umgang der in Kenntnis gesetzten Person mit dem betroffenen Migranten negativ beeinflussen. Dies gilt insbesondere für den Status im Asylverfahren oder die sensiblen Daten nach Art. 9 DS-GVO[73]. Die Offenlegung der Informationen an unbefugte Dritte stellt einen ernstzunehmenden Eingriff in die Freiheitsrechte des betroffenen Migranten dar. Dieser ist umso gewichtiger, je größer

---

70 ISO/TC 307/WG 2 – Working Group zu Security, privacy and identity (Blockchain and distributed ledger technologies).

71 DS-GVO, Erwägungsgrund 75.

72 DS-GVO, Erwägungsgrund 76.

73 Siehe hierzu bereits unter D.I.

die Zahl der potenziellen unberechtigten Empfänger der Daten und je größer der Datensatz ist.

b) Anzahl der betroffenen Personen und verarbeitenden Stellen

Beim geplanten Blockchain-Vorhaben sind ausschließlich personenbezogene Daten von Migranten betroffen. Im Jahr 2017 wurden 222.683 Asylanträge registriert, 2016 waren es 745.545.[74] Eine unberechtigte Offenlegung der Daten würde folglich eine Vielzahl von Personen betreffen.

Die Datenverarbeitung wird ausschließlich von öffentlichen Stellen vorgenommen. Anfangs sollen nur Aufnahmeeinrichtungen, das BAMF und die Ausländerbehörde Nürnberg Teil des Projekts sein. Mit zunehmender Verbreitung steigt jedoch die Zahl der beteiligten Stellen und Datenverarbeitungen. Angesichts der großen Zahl betroffener Personen ist bei der Implementierung daher besondere Vorsicht geboten.

c) Möglichkeiten einer Offenlegung der Daten

Die Offenlegung kann durch einen unbefugten Datenzugriff von außerhalb oder einer unbefugten Weitergabe innerhalb des Systems geschehen. Ein weiteres Risiko kann durch die Aufhebung der Pseudonymisierung gegeben sein.

(1) Unbefugter Datenzugriff

Die Daten werden in einer öffentlichen Blockchain gespeichert. Diese ist von jedermann einsehbar. Eine Kopie der Daten kann von jedermann jederzeit gezogen werden. Durch eine Verschlüsslung wird sichergestellt, dass personenbezogene Daten nicht lesbar sind. Die Verschlüsselung könnte jedoch gebrochen werden. Auf diese Weise wären zumindest die in der Blockchain eingespeicherten Daten für jedermann einsehbar. Die Zahl der hierdurch in Kenntnis gesetzten Personen kann im Falle eines veröffentlichten Datenleaks sehr groß sein. Durch Wahl einer geeigneten Verschlüsselung ist dieses Risiko aber effektiv zu minimieren. Wird die Verschlüsselung stets dem aktuellen Stand angepasst und auf hohem Niveau gehal-

74 *Bundesamt für Migration und Flüchtlinge*, Aktuelle Zahlen zu Asyl 04/2018, http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/Statistik/Asyl/aktuelle-zahlen-zu-asyl-april-2018.pdf?__blob=publicationFile, 5.4.

ten, so besteht für den unbefugten Datenzugriff durch Entschlüsselung nur ein sehr geringes Risiko.

Ein unbefugter Datenzugriff kann nicht nur auf die Daten in der Blockchain erfolgen, sondern auch auf die lokal eingespeicherten Daten auf den Systemen der öffentlichen Stellen. Auch diese sind gegen unbefugten Zugriff daher durch geeignete Mittel abzusichern. Es bietet sich auch für diese Daten zur Absicherung eine Verschlüsselung an.

(2) Unbefugte Weitergabe

Ein weiteres Risiko kann darin bestehen, dass eingespeicherte Daten für öffentliche Stellen sichtbar werden, die diese Daten nicht für die Erledigung ihrer Aufgaben benötigen. Dies kann dadurch geschehen, dass das implementierte Rechte- und Rollensystem den Zugriff in Einzelfällen auch dann erlaubt, wenn dies nicht vorgesehen ist. Hiervon sind Fälle der fehlerhaften Programmierung oder solche, bei denen eine Tatsache im Zeitpunkt der Programmierung noch nicht bekannt war, betroffen. Durch eine solche unbefugte Weitergabe sind lediglich andere öffentliche Stellen innerhalb des Systems betroffen. Das Risiko ist jedoch im Vergleich zum Aufbrechen der Verschlüsselung ungleich höher. Diesem Risiko muss daher durch Technikgestaltung begegnet werden.

(3) Aufhebung der Pseudonymisierung

Besteht für einzelne Beteiligte lediglich Einsicht in die On-Chain-Daten, nicht jedoch in die Off-Chain-Daten, so sind diese nur dann in der Lage die natürliche Person zu identifizieren, wenn ihnen die Aufhebung der Pseudonymisierung gelingt. Sie müssten daher von der On-Chain-Kennung des Migranten auf die natürliche Person schließen können. Das Risiko der Aufhebung hängt zum einen davon ab, welche Kennung in der Blockchain eingespeichert wird[75] und wer über den Schlüssel zur Verknüpfung der Informationen verfügt.

Wird die Off-Chain-Kennung auch auf der Blockchain verwendet, so ist eine Aufhebung der Pseudonymisierung wahrscheinlicher. Wird eine eigene Kennung verwendet, so hängt das Risiko von der Sicherung des Umrechnungsschlüssels ab. Wird hingegen auf die Speicherung

---

75 Siehe hierzu bereits unter E.III.

einer Kennnummer in der Blockchain gänzlich verzichtet, so besteht kein Risiko für eine Aufhebung der Pseudonymisierung.

3. Implementierungskosten

Art. 25 Abs. 1 DS-GVO schreibt eine Berücksichtigung der Implementierungskosten der technischen Maßnahmen vor. Dem Verantwortlichen muss die Implementierung wirtschaftlich zumutbar sein. Dabei müssen die Kosten ins Verhältnis zur Wirksamkeit der Maßnahme gestellt werden. Eine deutliche teurere Maßnahme wird nicht gefordert werden können, wenn durch sie die Wirksamkeit der Datensicherung nicht signifikant erhöht wird. Ist hingegen das Risiko für die Rechte und Freiheiten der Person erheblich, so sind entsprechend höhere Ausgaben vom Verantwortlichen zu fordern. Im Einzelfall kann dies auch dazu führen, dass von einer Datenverarbeitung abgesehen werden muss, wenn trotz zumutbarer Investitionen keine ausreichende Sicherheit gewährleistet werden kann.[76]

II. Technische und organisatorische Maßnahmen zur Wahrung der Datenschutzgrundsätze

Art. 25 Abs. 1 DS-GVO schreibt die Implementierung geeigneter technischer und organisatorischer Maßnahmen vor, die die Datenschutzgrundsätze wirksam umsetzen. Art. 25 Abs. 2 DS-GVO verdeutlicht, dass diese Implementierungen bereits durch Voreinstellungen bei der Konzeption der geplanten Datenverarbeitung umgesetzt werden müssen. Im Folgenden soll daher nicht zwischen den Absätzen differenziert, sondern anhand der Datenschutzgrundsätze des Art. 5 Abs. 1 DS-GVO untersucht werden, inwieweit sich diese bei der geplanten Datenübermittlung über eine Blockchain umsetzen lassen.

1. Transparenz, Art. 5 Abs. 1 lit. a

Beim Erfordernis der Transparenz muss zwischen der Transparenz über die Art und Weise der Datenverarbeitung einerseits und die Transparenz über die Informationen selbst unterschieden werden.[77] Dem Transparenzerfordernis wird in der Regel durch die Informationen nach den Art. 12 ff. DS-GVO nachgekommen. In diesen muss sowohl über die Art und Weise als auch über den Inhalt der Informationen berichtet werden.

---

76 Sydow/*Mantz*, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 25, Rn. 46.
77 Ehmann/Selmayr/*Heberlein*, EU-DS-GVO, 1. Aufl. 2017, Art. 5, Rn. 11.

Transparenz über den Inhalt der übermittelten Informationen ist in einer Public-Blockchain bereits von Natur aus gegeben. Im Falle des Einsatzes einer Permissioned-Blockchain sind die Informationen hingegen nur von einem eingeschränkten Personenkreis abrufbar. Letzteres ist auch im hier betrachteten Projekt geplant und sogar Voraussetzung für die Einhaltung der Datenschutzvorschriften. Die Betroffenen erhalten zunächst keinerlei Einblicke in die sie betreffenden gespeicherten und übermittelten personenbezogenen Daten.

Eine technische Möglichkeit zur Schaffung von Transparenz könnte die Programmierung einer Schnittstelle im Rechte- und Rollensystem zum Abruf der Daten durch den betroffenen Migranten sein. Auf diese Weise könnte jeder Migrant mit einer eigenen Kennung die ihn betreffenden personenbezogenen Daten abrufen und kontrollieren, an welche Empfänger diese übermittelt wurden.[78] Die Implementierung einer solchen Schnittstelle ist jedoch keinesfalls zwingend vorzunehmen. Dem Transparenzerfordernis kann auch durch Übermittlung der Informationen auf anderem Wege nachgekommen werden. Um diesen Pflichten nachzukommen, müsste der Verantwortliche aber jederzeit Zugriff auf alle über den Migranten gespeicherten Informationen haben.

Entscheidet man sich für die Implementierung einer Schnittstelle, so muss sowohl der technische und finanzielle Aufwand Beachtung finden. Durch die Zugriffsmöglichkeit der Migranten wird ein neues Risiko für eine unerlaubte Offenlegung der Daten geschaffen. Dies betrifft sowohl das Risiko einer technischen Anfälligkeit der Schnittstelle als auch das Risiko, das die Zugangsdaten in die Hände von Unbefugten geraten können. Diese Risiken sind bei einer Umsetzung ebenfalls mit in die Erwägung einzubeziehen.

2. Zweckbindung, Art. 5 Abs. 1 lit. b

Die Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer, mit diesen Zwecken nicht zu vereinbarenden Weise, weiterverarbeitet werden. Die Datenübermittlung ist als Weiterverarbeitung zuvor zweckbedingt erhobener Daten zu verstehen. Dabei besteht der Zweck des Austausches der Daten zwischen den öffentlichen Stellen bereits bei Datenerhebung. Die Daten sind jedoch nur denjenigen öffentlichen Stellen zugänglich zu machen, die sie für die Erledigung ihrer Aufgaben benötigen.

---

78 So auch *Guggenberger*, Datenschutz durch Blockchain – eine große Chance, ZD 2017, 49 (50).

Dem Erfordernis der Zweckbindung bei Weitergabe der Daten kann theoretisch durch Technikgestaltung genügt werden. Dies erfordert jedoch, dass das Rechte- und Rollensystem autonom erkennt, wann Daten für die Erledigung der Aufgaben einer konkreten öffentlichen Stelle erforderlich sind. Nur so kann es entscheiden, welchen öffentlichen Stellen Leserechte für die gespeicherten Daten gewährt werden dürfen. Die Normen des AZRG können als Grundlage für die Programmierung des Systems dienen. Eine Herausforderung wird es hingegen darstellen, alle Entscheidungen über die Erforderlichkeit durch die Software treffen zu lassen. Es ist daher nicht auszuschließen, dass für Zweifelsfälle eine Schnittstelle für den Verantwortlichen geschaffen werden muss, bei welchem eine natürliche Person im Verantwortungskreis des Verantwortlichen über die Erforderlichkeit der Datenübermittlung entscheiden muss.

3. Datenminimierung, Art. 5 Abs. 1 lit. c

Die Datenverarbeitung soll stets auf das für die Verarbeitung erforderliche Maß beschränkt werden. Hierzu zählt die Anonymisierung und Pseudonymisierung von Daten, soweit dies möglich ist, sowie der Verzicht auf die Speicherung unnötiger Daten.

a) Anonymisierung und Pseudonymisierung

Art. 4 Nr. 5 DS-GVO definiert Pseudonymisierung als eine „Verarbeitung personenbezogener Daten in einer Weise, dass 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 und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden". Auch Daten, die einer Pseudonymisierung unterzogen wurden, sind personenbezogene Daten.[79] Es handelt sich in diesem Fall um indirekt bestimmbare Informationen über eine natürliche Person.[80] Durch die Pseudonymisierung werden andere Datenschutzmaßnahmen nicht ausgeschlossen.[81] Sie senkt lediglich die Risiken für die be-

79 DS-GVO, Erwägungsgrund 26 S. 2.
80 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 21.
81 DS-GVO, Erwägungsgrund 28 S. 2.

troffene Person identifiziert zu werden. Verantwortliche und Auftragsverarbeiter werden durch sie bei der Einhaltung ihrer Pflichten unterstützt.[82]

Durch die Verwendung einer Kennnummer ist die natürliche Person (Migrant) nicht mehr direkt identifizierbar. Nur durch Hinzuziehen von Informationen ist ein Personenbezug herzustellen. Diese Informationen werden gesondert gespeichert. Bei bloßer Einsicht der in der Blockchain eingespeicherten Daten ist daher ohne Kenntnis des Schlüssels zwischen Kennnummer und Migrant eine Identifizierung nicht möglich. Folglich handelt es sich bei der Kennnummer um ein Pseudonym.

In Abgrenzung zu pseudonymen Daten sind anonyme Daten solche, die sich zwar auf eine natürliche Person beziehen, diese jedoch weder von dem für die Verarbeitung Verantwortlichen noch einem Dritten bestimmt werden kann.[83] Eine Einordnung hat im Einzelfall danach zu erfolgen, ob Mittel bereitstehen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.[84]

Eine Anonymisierung der übermittelten Daten ist im geplanten Blockchain-Verfahren grundsätzlich nicht denkbar. Die Identifizierung der natürlichen Personen ist gerade Voraussetzung für die Nutzung der Daten durch die öffentlichen Stellen. Wäre den Verantwortlichen die Identifizierung der Person nicht möglich, so könnten die Daten für den vorgesehenen Zweck nicht verwertet werden.

b) Keine Speicherung unnötiger Daten

Bei der Verwendung einer Blockchain werden die Daten redundant gespeichert. Dies könnte dem Grundsatz der Datenminimierung widersprechen, da die mehrfache Speicherung der Daten bei Anwendung einer anderen Übermittlungsmethode nicht zwingend notwendig wäre. Es kommt jedoch beim Grundsatz der Datenminimierung auf den Informationswert der

---

82 DS-GVO, Erwägungsgrund 28 S. 1.
83 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 24.
84 DS-GVO, Erwägungsgrund 26 S. 3.

Daten und nicht auf die Anzahl der vorhandenen Kopien an. Eine mehrfache Speicherung derselben Daten steht dem Grundsatz der Datenminimierung folglich nicht entgegen. [85]

Die in die Blockchain eingespeicherten Daten sind rückwirkend grundsätzlich nicht löschbar.[86] Demzufolge muss der Grundsatz der Datenminimierung gerade für diese Informationen im besonderen Maße gelten. Soweit die technische Umsetzbarkeit des Vorhabens auch durch einen Verzicht auf die Speicherung von Kennnummer, Status, bearbeitender öffentlicher Stelle und Zeitstempel mit vertretbarem Aufwand möglich ist,[87] ist eine solche Lösung vor dem Hintergrund des Grundsatzes der Datenminimierung vorzuziehen.

4. Richtigkeit der Daten und Speicherbegrenzung, Art. 5 Abs. 1 lit. d und e

Die verarbeiteten personenbezogenen Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Unrichtige Daten sind durch geeignete Maßnahmen unverzüglich zu löschen oder zu berichtigen. Zudem müssen sie in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Die Einpflegung der Daten in eine Blockchain ermöglicht durch die verteilte Speicherung einen ständigen Abgleich der Daten. Hierdurch können nachträgliche Manipulationen verhindert werden.[88] Es kann hingegen nicht sichergestellt werden, dass die eingespeicherten personenbezogenen Daten auch richtig sind. Ursprünglich falsch eingepflegte Daten werden unveränderbar gespeichert. Es ist daher ein Löschkonzept für die personenbezogenen On-Chain-Daten zu entwickeln.[89]

5. Vertraulichkeit, Art. 5 Abs. 1 lit. f Var. 2

Die personenbezogenen Daten müssen vertraulich behandelt werden. Dies erfordert, dass unbefugte Personen keinen Zugriff auf die Daten erhalten. In einer Public-Blockchain ist diese Vertraulichkeit für die eingepflegten Daten nicht gegeben, da sie von jedermann einseh-

---

85 So auch *Marnau*, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, Informatik 2017, 1025 (1029); a.A. *Finck*, Blockchain and Data Protection in the European Union, EDPL 1/2018, 17 (28f.).

86 Ausnahme stellt die Redactable Blockchain dar. Siehe dazu bereits unter E.III.1.

87 Siehe dazu bereits unter E.III.3.

88 Hierzu auch *Bechtolf/Vogt*, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66 (67).

89 Möglichkeiten hierzu wurden bereits unter E.III. diskutiert.

bar sind. In der geplanten Permissioned-Biockchain werden die Leserechte zentral vergeben. Hierdurch kann die Vertraulichkeit der Daten gewährleistet werden. Es sind dabei geeignete technische Maßnahmen zu treffen, die eine Umgehung der Berechtigungsvoraussetzung verhindern.

6. Integrität, Art. 5 Abs. 1 lit. f Var. 1

Personenbezogene Daten sind vor unbefugter Manipulation zu schützen. Hierfür bietet der Einsatz einer Blockchain starke Garantien. Einmal eingespeicherte Daten sind nachträglich nicht veränderbar.[90] Auf diese Weise kann die Integrität der On-Chain-Daten gewährleistet werden. Die Off-Chain-Daten könnten hingegen durch die einpflegende öffentliche Stelle, auf deren System sie sich befinden, oder durch externe Angreifer manipuliert werden. Hiergegen sind von Seiten der öffentlichen Stellen oder durch eine Zentralstelle geeignete Maßnahmen zu ergreifen. Eine solche könnte die Einspeicherung eines Hash-Werts der Off-Chain-Daten in der Blockchain sein.[91]

Neben der Manipulation sind die Daten auch vor unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung zu schützen. Auch hierfür bietet die Blockchain, durch die redundante Speicherung, zunächst gute Voraussetzungen. Ein Risiko könnte hingegen in der Implementierung auf Basis einer Public-Biockchain liegen. Durch die Nutzung der Ethereum-Biockchain macht sich das Projekt von deren Schicksal abhängig. Kommt es zu Fehlern in der Ethereum-Biockchain oder kommt das öffentliche Projekt gar zum Erliegen, so würde daran auch die weitere Datenübermittlung scheitern.

Die Integrität der Daten wird jedoch dadurch gesichert, dass diese auf den lokalen Systemen der öffentlichen Stellen verbleiben, welche vom Schicksal der Public-Biockchain unabhängig sind. Folglich stellt die Verwendung einer Public-Blockchain als Basis zunächst keinen Widerspruch zur Integrität der Daten dar. Dennoch ist das Konzept einer Public-Blockchain als Basis langfristig zu hinterfragen. Zwar ist dies bei sicherer Verschlüsselung für den Datenschutz unerheblich, die Abhängigkeit kann aber trotzdem zu einem Scheitern des Projekts führen.

---

90 So auch *Bechtolf/Vogt*, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66 (67); Eine Ausnahme besteht nur bei einem Angriff auf den jeweiligen Konsens-Mechanismus der Blockchain, z.B. 51%-Attacke bei Proof-of-Work. Dies soll jedoch hier außer Acht bleiben.

91 Siehe hierzu bereit unter E.III.3.

III. Zwischenfazit

Der geplante Datenaustausch zwischen den öffentlichen Stellen birgt, aufgrund der großen Anzahl betroffener Personen, des Umfang der übermittelten Datensätze und der voraussichtlich wachsenden Zahl verarbeitender Stellen ein beachtliches Risiko für die Rechte und Freiheiten der betroffenen Personen. Aus diesem Grund sind bei der Implementierung von technischen Maßnahmen zur Wahrung der Betroffenenrechte bei der Datenverarbeitung auch erhebliche Implementierungskosten in Kauf zu nehmen.

Technische Maßnahmen zur Wahrung der Betroffenenrechte können grundsätzlich auch durch eine Blockchain-Lösung getroffen werden. Die Blockchain entspricht als eine Alternative zur zentralen Datenspeicherung dem aktuellen Stand der Technik. Zur Schaffung von Transparenz ist eine Schnittstelle für die Einsicht der Daten durch die Betroffenen denkbar, aber nicht zwingend.

Für die Gewährleistung der Richtigkeit der Daten und der Begrenzung der Speicherung für nicht mehr erforderliche Daten sind geeignete Maßnahmen zu treffen. Solche können beispielsweise die Erstellung eines später zu löschenden Umrechnungsschlüssels, der Einsatz einer Redactable Blockchain oder der Verzicht auf die Speicherung aller personenbezogenen Daten in der Blockchain sein. Mit letzterer Maßnahme würde auch dem Grundsatz der Datenminimierung bestmöglich genügt. Dieser erfordert jedenfalls die konsequente Pseudonymiserung durch Verwendung von Kennnummern.

Für die Integrität von Daten ist der Einsatz einer Blockchain zunächst vielversprechend. Die Vorteile der Blockchain sollten jedoch auch für die Off-Chain-Daten genutzt werden, wofür über die Einspeicherung eines Hash-Werts der lokal bei den öffentlichen Stellen verbleibenden Daten nachgedacht werden könnte. Eine Vertraulichkeit der Daten kann durch ein zuverlässiges Rechte- und Rollensystem geschaffen werden. Dieses Rechte- und Rollensystem steht vor dem Hintergrund des Grundsatzes der Zweckbindung vor der Herausforderung, die Leserechte stets nur denjenigen öffentlichen Stellen zu ermöglichen, welche die Daten für die Erledigung ihrer Aufgaben benötigen. Im Zweifel bietet sich die Implementierung einer Schnittstelle zur Überprüfung von Einzelfällen an.

G. Zusammenfassung der Ergebnisse

Der geplante Einsatz einer Permissioned-Blockchain zum Austausch von Informationen über registrierte Migranten zwischen den am Asylverfahren beteiligten öffentlichen Stellen ist de lege lata - mit Ausnahme der Übermittlung sensibler Daten nach Art. 9 DS-GVO - grundsätzlich datenschutzrechtlich zulässig. Ein zwingender Anpassungsbedarf besteht hinsichtlich der Ausarbeitung eines Löschkonzepts für die in der Blockchain eingespeicherten personenbezogenen Daten. Eine Herausforderung stellt die datenschutzrechtskonforme Programmierung des Rechte- und Rollensystems dar.

Beim geplanten Verfahren finden sowohl bei der Einpflegung der Daten als auch beim Auslesen der Daten durch die öffentlichen Stellen Datenverarbeitungen statt. Verantwortlicher für das Auslesen der Daten ist die jeweils auslesende öffentliche Stelle. Die Verantwortlichkeit für die Einpflegung der Daten kann entweder eine Zentralstelle alleine oder die einpflegende öffentliche Stelle gemeinsam mit der Zentralstelle übernehmen. Soll die einpflegende öffentliche Stelle die alleinige Verantwortliche sein, so muss die Vergabe der Berechtigungen im Rechte- und Rollensystem allein in ihre Hände gelegt werden. Bei den verarbeiteten Daten handelt es sich sowohl bei den Off-Chain-Daten als auch, nach dem bisherigen Konzept, bei den On-Chain-Daten, aufgrund der Identifizierbarkeit des Migranten durch die Kennnummer, um personenbezogene Daten.

Die Verarbeitung personenbezogener Daten ist rechtfertigungsbedürftig. Ein Rechtfertigungsgrund findet sich in Art. 6 Abs. 1 lit. e DS-GVO. Dieser erfordert jedoch eine weitere Rechtsgrundlage aus dem Unionsrecht oder dem Recht der Mitgliedsstaaten. Das AZRG ist insoweit nicht anwendbar, da es auf den Spezialfall des Ausländerzentralregisters zugeschnitten ist. Eine Rechtfertigung für die Übermittlung von Daten zwischen öffentlichen Stellen findet sich in § 25 Abs. 1 BDSG neu. Dieser erlaubt die Datenübermittlung, soweit sie für die Erledigung der Aufgaben der übermittelnden oder empfangenden öffentlichen Stelle erforderlich ist. Die Frage der Erforderlichkeit muss im Einzelfall vom Verantwortlichen geprüft werden. Dies kann grundsätzlich auch durch die Software des Rechte- und Rollensystems geschehen, wobei insbesondere Zweifelsfälle eine Herausforderung darstellen können.

Geht man davon aus, dass Daten, die bislang nach § 3 AZRG im Ausländerzentralregister gespeichert wurden, übermittelt werden sollen, so handelt es sich bei den Informationen über

die Religionszugehörigkeit und die Fingerabrücke, den Gesundheitsdaten und den Daten über gesundheitliche Maßnahmen um sensible Daten nach Art. 9 DS-GVO. Eine Rechtfertigung deren Übermittlung über eine Blockchain ist de lege lata nicht möglich. Insbesondere dient die geplante Verarbeitung nicht Archivzwecken im öffentlichen Interesse, Forschungszwecken oder statistischen Zwecken. Eine Rechtfertigungsnorm im nationalen Recht, die den Anforderungen an Art. 9 Abs. 2 lit. g DSVGO genügt, findet sich derzeit nicht.

Die Wahrung der Betroffenenrechte nach der DS-GVO ist auch beim Einsatz einer Datenübermittlung über die Blockchain möglich. Anpassungsbedarf besteht jedoch hinsichtlich des Rechts auf Berichtigung falscher und Löschung nicht mehr benötigter Daten.

Die Blockchain-Lösung bietet Möglichkeiten für eine Datenschutzstrategie durch Technik nach Art. 25 DS-GVO. Herausforderungen sind dabei die Gestaltung des Rechte- und Rollensystems zur Gewährleistung der Zweckbindung bei der Datenverarbeitung und die bereits angesprochene Ausarbeitung eines Löschkonzepts für unrichtige oder nicht mehr benötigte Daten.