NutriSafe

Sicherheit in der Lebensmittelproduktion und -logistik
durch die Distributed-Ledger-Technologie

IGMR

NutriSafe Toolkit

– Rechtlicher Rahmen –

Blockchains für Versorgungsketten im Lebensmittelsektor und der Datenschutz

Die Maßstäbe für eine datenschutzkonforme Ausgestaltung der Blockchain am konkreten Beispiel

Dr. Dennis-Kenji Kipker – Hauke Bruns

Aufsatz aus:

Computer und Recht - Zeitschrift für die Praxis des Rechts der Informationstechnologie
2020/3, 36. Jahrgang

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Bundesministerium Landwirtschaft, Regionen und Tourismus

SIFO.de

KIRAS Sicherheitsforschung

FFG Forschung wirkt.

3 | 2020

36. Jahrgang
15. März 2020
S. 145–216

PVSt 9892

CR

Computer und Recht

Zeitschrift für die Praxis des Rechts der Informationstechnologie

cr-online.de

ottoschmidt

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Ist die Verwendung der Klauseln Ziff. 7.4 S. 2 und Ziff. 7.5 S. 2 der Allgemeinen Bedingungen bereits deshalb zu untersagen, weil sie hinsichtlich der Voraussetzungen einer Leistungsabschaltung § 45k II TKG nicht berücksichtigen, kann dahingestellt bleiben, ob die Beklagte als Rechtsfolge einer sonst etwa berechtigten Leistungsabschaltung die Kosten dieser und der (nach Rückstandsausgleich durchgeführten) Freischaltung des Anschlusses als pauschalierten Aufwendungs- oder Schadenersatz erstattet verlangen kann (vgl. dazu nur *Arndt/Fetzer/Scherer/Graulich/Lutz*, TKG, 2, Aufl. 2015, § 45k Rz. 45; offen gelassen von BGH, Urt. v. 18.4.2002 – III ZR 199/01, CR 2002, 658 m. Anm. *Heun* = juris Rz. 29). (...)

OVG NW: Bestimmtheitsanforderungen an Untersagungsverfügung wegen unerlaubter Telefonwerbung

UWG § 7; TKG § 67; VwVfg §§ 6, 44, 37; VwGO § 86

Eine von der Bundesnetzagentur erlassene Untersagungsverfügung, mit der dem Betroffenen verboten wird, „Werbung mit Telefonanrufen gegenüber Verbrauchern selbst durchzuführen oder durch Dritte durchführen zu lassen, wenn die Angerufenen im Vorfeld nicht gesetzeskonform in den Erhalt derartiger Telefonwerbung eingewilligt haben", wird angesichts der in der Rechtsprechung ungeklärten Frage, unter welchen Umständen eine den Anforderungen des § 7 Abs. 2 Nr. 2 Alt. 1 UWG genügende Einwilligung vorliegt, den Bestimmtheitsanforderungen des § 37 Abs. 1 VwVfG nicht gerecht.

(nicht amtl.)

OVG NW, Beschl. v. 22.10.2019 – 13 B 600/19 (rkr.)
(VG Köln, Beschl. v. 12.4.2019 – 9 L 1706/18)

Report und Technik

Aufsätze

Dennis-Kenji Kipker / Hauke Bruns*

Blockchains für Versorgungsketten im Lebensmittelsektor und der Datenschutz

Die Maßstäbe für eine datenschutzkonforme Ausgestaltung der Blockchain am konkreten Beispiel

Jeder Fall verunreinigter Lebensmittel lässt die Forderungen nach deren Rückverfolgbarkeit und die Verfügbarkeit der dabei generierten Daten aufs Neue laut werden. Die Rückverfolgbarkeit erfordert die Erhebung von Daten, die eine Zuordnung der Produkte zu Vertriebsstellen, Logistikrouten, Produktionsstandorten und Produktionszeitpunkten ermöglichen. Wird dann wegen einer Qualitätskontrolle, oder aber aufgrund eines erkrankten Endverbrauchers, eine Unregelmäßigkeit erkannt, so ist anhand dieser Daten eine Ermittlung der Fehlerquelle möglich und weitere, u.U. ebenfalls betroffene Produkte können gefunden und deren Wege in der Lieferkette nachvollzogen werden. Um in einem solchen Fall zeitnah zu reagieren, ist die Verfügbarkeit der Daten notwendig. Zudem ist die technisch-organisatorische Absicherung der Datenbestände vor Angriffen erforderlich, um ihre Integrität sicherzustellen. Hierzu bietet sich als technisches Instrument zur Umsetzung die Distributed Ledger Technologie (DLT) an.

I. Einsatz und Funktionsweise der DLT

Ein praktisches Einsatzszenario der DLT im Lebensmittelsektor ist die Herstellung von Käsereiprodukten: Der Produktionsprozess beginnt mit dem Melken der Kühe beim Milcherzeuger. Anschließend wird die Milch vom Spediteur zur Molkerei gebracht, in der sie dann zu Käseprodukten verarbeitet wird und diese verpackt werden. Eine bereits nach dem Melken genommene Probe der Milch wird währenddessen im Labor untersucht. Ein weiterer Spediteur liefert das fertige Produkt schließlich an einen Großhändler, der seinerseits die Ware an den Supermarkt liefert, der sie auslegt und verkauft. Dieses Beispiel zeigt, dass eine Absicherung der Kette von der Milcherzeugung bis zum Verkauf, wegen der Vielzahl der beteiligten Akteure und Verarbeitungsschritte, die Aufzeichnung von Daten zu den Produkten, aber auch den Personen erfordert, die mit der Her- 1

* Dieser Beitrag entstand im Rahmen des vom BMBF-geförderten Forschungsprojekts „NutriSafe" – Sicherheit in der Lebensmittelproduktion und -logistik durch die Distributed-Ledger-Technologie.

stellung und Prüfung befasst sind. Bei einer näheren Betrachtung der Vielzahl verarbeiteter Daten ergeben sich verschiedene datenschutzrechtliche Probleme, die sich auf die Absicherung von Versorgungsketten im Allgemeinen und die Verwendung der DLT im Speziellen beziehen.

2 Von klassischen Datenbanken grenzt sich die DLT dadurch ab, dass die Datensätze dezentral gespeichert werden. Das bedeutet, dass anstelle einer zentralen Stelle die einzelnen, an dem System beteiligten Akteure einen neuen Datensatz hinzufügen können. Dieser wird dann im Verzeichnis eines jeden an der DLT Beteiligten gespeichert. Die Einheitlichkeit der in den unterschiedlichen Verzeichnissen gespeicherten Daten wird dadurch erreicht, dass ein jeder Eintrag zuvor nach einem festgelegten Verfahren überprüft wird. Das Prüfverfahren, an dessen Ende ein Konsens über den zu speichernden Datensatz steht, unterscheidet sich je nach Ausgestaltung der DLT. Bei sog. „*permissioned*" Ledgers ist dies oftmals der sog. „proof-of-stake", bei „*unpermissioned*" Ledgers meist der sog. „proof-of-work".[1] Trotz mitunter synonymer Verwendung der Begriffe ist die sog. „Blockchain" letztlich eine Form der Ausgestaltung der DLT, genauer eines unpermissioned Ledgers. Hierbei werden die zu speichernden Informationen eines Ereignisses jeweils in einem Block zusammengefasst und die einzelnen Blöcke aneinandergehängt. Eine Änderung eines Blocks bedarf deshalb der Änderung aller folgenden (angehängten) Blöcke, womit die Änderung ab einer gewissen Anzahl nachfolgender Blöcke faktisch ausgeschlossen ist.[2] Im Logistik[3]- und Lebensmittelsektor[4] hat die Blockchain-Technologie bereits in erste Projekte Einzug gehalten.

II. In der DLT zu speichernde Datenkategorien

1. Daten aus gesetzlichen Anforderungen an die Rückverfolgbarkeit von Lebensmitteln

3 Gesetzliche Aufzeichnungspflichten im Lebensmittelsektor ergeben sich aus der VO EG 178/2002[5] sowie dem Lebensmittel- und Futtermittelgesetzbuch (LFGB), das ergänzende Regelungen enthält. Die VO EG Nr. 178/2002 („VO") statuiert für Lebensmittel- und Futtermittelunternehmer eine Verpflichtung, die Rückverfolgbarkeit zu gewährleisten. Rückverfolgbarkeit meint gem. Art. 3 Nr. 15 der VO die Möglichkeit, den Weg eines Lebensmittels durch alle Produktions-, Verarbeitungs- und Vertriebsstufen nachzuvollziehen. Die Lebensmittelunternehmer trifft hierzu nach Art. 18 der VO die Pflicht, jede Person feststellen zu können, von der sie ein Lebensmittel erhalten haben (Abs. 2 Unterabs. 1) sowie jene Unternehmen, an die sie solche geliefert haben (Abs. 3). Sie haben außerdem gem. Art. 18 Abs. 2 Unterabs. 2 der VO Systeme und Verfahren einzurichten, die ihnen die Übermittlung dieser Informationen an die zuständigen Behörden ermöglichen, woraus sich faktisch eine Pflicht zur Mitteilung ergibt.[6]

4 Im nationalen Recht konkretisiert § 44 Abs. 3 S. 1 LFGB diese Verpflichtung. Dessen S. 2 schreibt für in elektronischer Form vorliegende Daten die Verpflichtung zur Übermittlung gemäß dem beschriebenen Verfahren vor. Bezweckt wird damit die alsbaldige Verfügbarkeit der Daten für die Aufsichtsbehörden.[7] Eine Anpassung des § 44 Abs. 3 LFGB, die Bereitstellung der Informationen zwingend in elektronischer und einheitlicher Form sowie binnen 24 Stunden vorzuschreiben, wird zwar von der Verbraucherschutzministerkonferenz gefordert,[8] ist derzeit aber (noch) nicht vorgesehen.

Die Pflicht zur Mitteilung der Lieferanten- und Kundendaten indiziert eine Pflicht zur Aufzeichnung.[9] Inhaltlich muss die Aufzeichnung die Rückverfolgbarkeit eines Lebensmittels ermöglichen. Es müssen deshalb sowohl die Lieferantendaten (einschließlich Adresse) sowie Daten zur gelieferten Ware (Datum, Chargennummer, Menge) vermerkt sein. Gleiches gilt für die Weitergabe an Abnehmer. Ob es sich bei den Lieferanten um natürliche oder juristische Personen handelt, ist unbeachtlich. Lediglich bei der Weitergabe an private Endverbraucher entfällt eine Pflicht zur Aufzeichnung.[10] 5

2. Daten zur Qualitätssicherung

Um die Qualität der Lebensmittel zu gewährleisten, sind über die gesetzlichen Anforderungen hinaus weitere Daten zum Produkt zu erheben und zu speichern. Die zur Sicherung der Qualität zu speichernden Daten stammen aus zwischen den Verarbeitungsschritten und Transportabschnitten fortwährend durchgeführten Qualitätskontrollen. Die Speicherung der Daten im Blockchain-Verzeichnis ermöglicht zum einen, dass die übrigen Teilnehmer – bspw. die Abnehmer – die Durchführung der Kontrollen und die dabei festgestellten Werte einsehen können. Zum anderen ist eine nachträgliche Änderung der einmal gespeicherten Daten nicht möglich. Bezogen auf die eingangs dargestellte Käseherstellung kann die Milch damit bereits zur Molkerei transportiert werden, mit der Verarbeitung hingegen bis zum Ende der Laboruntersuchung und der folgenden Eintragung der Laborergebnisse in die Blockchain gewartet werden. Die Werte geben Aufschluss über die Zusammensetzung der Milch und evtl. enthaltene Krankheitserreger. Die Entnahme und Untersuchung der Proben erfolgt durch einen Mitarbeiter, der die Ergebnisse anschließend einträgt und abzeichnet. 6

1 https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444 (3.1.2020).

2 https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-277215 (3.1.2020).

3 https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/krypto-kolumne/coin-und-co-die-krypto-kolumne-wieso-die-logistik-ein-geeignetes-einsatzgebiet-der-blockchain-ist/22898364.html (3.1.2020).

4 https://www.lebensmittelverband.de/de/aktuell/20180822-blockchain-fuer-rueckverfolgbarkeit-und-lebensmittel-sicherheit-entlang-der-kette-food-branche (3.1.2020).

5 Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28.1.2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit.

6 *Boch,* Nomos-BR LFGB, 8. Online-Aufl. 2019, LFGB § 44 Rz. 3.

7 *Boch,* Nomos-BR LFGB, 8. Online-Aufl. 2019, LFGB § 44 Rz. 3.

8 Ergebnisprotokoll der 9. Verbraucherschutzministerkonferenz am 17.5.2013 in Bad Nauheim, Top 15, S. 24.

9 *Rathke* in Zipfel/Rathke LebenmittelR, EG-Lebensmittel-Basisverordnung, 173. EL 03/2019, Art. 18 Rz. 6 ff.

10 *Rathke* in Zipfel/Rathke LebenmittelR, EG-Lebensmittel-Basisverordnung, 173. EL 03/2019, Art. 18 Rz. 18.

3. Standortdaten

7 Außerdem können über die gesetzlich zur Rückverfolgbarkeit von Lebensmitteln geforderten Daten hinaus auch Standortdaten erfasst und gespeichert werden. Aus den Standortdaten eines Transportfahrzeugs (bspw. mittels GPS) lassen sich die Transportwege der Produkte feststellen. Im Rahmen einer auch für den Kunden (in Teilen) einsehbaren Blockchain profitiert dieser von den Informationen über die Transportwege eines Produkts, da sich aus diesen mittelbar Rückschlüsse auf die Herkunft und die für den Transport eingesetzten Ressourcen ziehen lassen.

III. Personenbezug der zu verarbeitenden Datenkategorien

8 Inwieweit die zuvor aufgezeigten Informationen den Anforderungen des Datenschutzrechts unterliegen, hängt zuvorderst von der Eröffnung des sachlichen Anwendungsbereichs der DSGVO ab. Entscheidend ist dabei, ob personenbezogene Daten vorliegen. Dies folgt schon aus Art. 2 Abs. 1 DSGVO. Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

1. Daten aus gesetzlichen Anforderungen

9 Um den Vorgaben aus der VO (EU) Nr. 178/2002 gerecht zu werden, ist die Speicherung der Lieferanten- und Kundendaten vorzunehmen, insoweit folglich Angaben zu Name/Firmenname und Adresse. Soweit es sich bei den Unternehmen ausschließlich um juristische Personen handelt, deren Daten gespeichert werden, ist dies auf den ersten Blick datenschutzrechtlich unbedenklich, da es hierbei grundsätzlich an einem Bezug zu natürlichen Personen mangelt und damit keine personenbezogenen Daten i.S.d. Art. 4 Nr. 1 DSGVO vorliegen.[11] Reine Unternehmensdaten unterfallen folglich nicht dem Anwendungsbereich der DSGVO.[12] Enthält die Bezeichnung der juristischen Person jedoch Namen der (natürlichen) Gesellschafter, so weisen die Informationen einen Personenbezug zu einer natürlichen Person auf,[13] soweit sie Rückschlüsse auf die finanziellen oder wirtschaftlichen Verhältnisse eben dieser zulassen[14]. Gleiches gilt für Personengruppen oder Personenmehrheiten wie etwa Personengesellschaften.[15] Zum Teil wird unter Hinweis auf ErwGr Nr. 14 S. 2 zur DSGVO, der den Namen einer juristischen Person bewusst ausnimmt, gefordert, die Annahme eines Personenbezugs insoweit aber auf Fälle zu beschränken, in denen die Verarbeitung „erkennbar auf die im Firmennamen benannten natürlichen Personen abzielt."[16] Mit Blick auf die Eigenart einer „Ein-Mann-GmbH", unter gleichzeitiger Berücksichtigung des genannten Ausschlusses juristischer Personen (EG. 14 S. 2 DSGVO), kann die Annahme eines Personenbezugs grundsätzlich unter diesen Vorbehalt gestellt werden.

10 Speziell für den Lebensmittelsektor ist aber eine Besonderheit zu berücksichtigen: Von erheblicher Bedeutung ist hier der Primärsektor (die sog. „*Urproduktion*"), zu dem etwa landwirtschaftliche Betriebe zählen. Diese firmieren überwiegend nicht als juristische Personen, sondern zu einem weit überwiegenden Teil als Einzelunternehmer.[17] Gleiches gilt für den Tertiärsektor, zu dem der Groß- und Einzelhandel zählt – auch hier sind nicht selten eingetragene Kaufleute anzutreffen. Für deren Daten ergibt sich der Personenbezug entweder bereits aus ihrer Eigenschaft als natürliche Person oder aber jedenfalls dadurch, dass unternehmensbezogene Daten notwendigerweise auf sie als einzige dahinterstehende Person bezogen werden können, beispielsweise über die Bezeichnung oder Anschrift eines landwirtschaftlichen Betriebs oder Lebensmittelhandels. Ganz ähnliche Erwägungen müssen für den Logistiksektor angestellt werden, denn auch hier kommt es nicht selten vor, dass beispielsweise kleine Spediteure als Ein-Mann-Betriebe unter ihrem eigenen Namen firmieren. Anders als bei juristischen Personen lassen die Daten hier nicht bloß ausnahmsweise Rückschlüsse auf die dahinterstehenden Personen zu.

2. Standortdaten und Daten aus der Qualitätskontrolle

11 Standortdaten weisen grundsätzlich eine datenschutzrechtliche Relevanz auf, denn soweit sie einer natürlichen Person zugeordnet werden können, handelt es sich um ein personenbezogenes Datum.[18] Werden die Standortdaten unter dem *Grundsatz der Datenminimierung* (Art. 5 Abs. 1 lit. c DSGVO) ohne Verknüpfung zu einer konkreten Person – etwa dem Kraftfahrer – gespeichert, weisen sie jedoch keinen Bezug zu einer bereits identifizierten natürlichen Person auf. Gleichwohl könnte die Person unter Zuhilfenahme weiterer Informationen – etwa eines Dienst- oder Einsatzplans – identifizierbar sein.

12 Auch Daten aus der Qualitätskontrolle – z.B. dass ein bestimmter Kontrolleur eine Kontrolle durchgeführt hat – sind personenbezogene Daten. Werden die Durchführung der Kontrolle bzw. Daten aus der Kontrolle in der Blockchain gespeichert, kann ein Interesse bestehen, diese Daten einem konkreten Kontrolleur zuordnen zu können. Mit Blick auf den Grundsatz der Datenminimierung sollte jedoch auch hier auf die Nennung des Klarnamens des Kontrolleurs in der Blockchain verzichtet werden. Stattdessen ist die jeweilige Kontrolle einer Kennung zuzuordnen, die ihrerseits dann lediglich über eine Liste außerhalb der Blockchain einem Klarnamen zugeordnet werden kann. Aus dem personenbezogenen Qualitätskontrolldatum wird dadurch ein gem. Art. 4 Nr. 5 DSGVO pseudonymisiertes, also ein solches Datum, das ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Per-

11 So ausdr. EG 14, der „Daten juristischer Personen und insbesondere als juristische Person [...] einschließlich Name, Rechtsform oder Kontaktdaten" ausnimmt.

12 *Ernst* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Rz. 6.

13 *Ernst* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Rz. 5; *Gola* in Gola, DSGVO, 2. Aufl. 2018, Art. 4 DSGVO Rz. 25, der dies für den Namen und damit verbundene Adressdaten verneint, in Fällen einer engen Verflechtung aber gleichwohl einen Bezug der Angaben zu den dahinterstehenden natürlichen Personen sieht, so dass sie als personenbezogene Daten anzusehen seien.

14 *Klar/Kühling* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Nr. 1 Rz. 4.

15 *Klar/Kühling* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Nr. 1 Rz. 4; *Arning/Rothkegel* in Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO Nr. 1 Rz. 16.

16 *Saive/Janicki*, RdTW 2019, 201 (204).

17 Landwirtschaftliche Betriebe gar zu gut 89 Prozent (2016), https://www.bauernverband.de/34-betriebs-rechtsformen (3.1.2020).

18 *Weichert*, DuD, 2007, 113 (114).

son zugeordnet werden kann. Die Pseudonymisierung bewirkt bei gleichzeitigem Zugriff auf die Zuordnungsregeln jedoch keine *Anonymisierung* der Daten, so dass die Daten in diesem Fall nach wie vor personenbezogene Daten darstellen[19] und damit dem Regelungsregime der DSGVO unterfallen.

13 Da jeder Akteur mit Zugriff auf die Blockchain zunächst (nur) auf die in der Blockchain gespeicherten Standortdaten und Qualitätskontrolldaten sowie Kennungen der Kontrolleure zugreifen kann, sind zur Identifizierung im Regelfall weitere Mittel erforderlich. Nach EG 26 S. 3 zur DSGVO sollen i. R. d. Beurteilung der Identifizierbarkeit alle solche Mittel berücksichtigt werden, die vom Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden. EG 26 S. 4 zur DSGVO konkretisiert, dass für diese Beurteilung *alle* objektiven Faktoren zu berücksichtigen sind, wozu etwa Kosten, Zeitaufwand und die verfügbare Technologie zählen. Betrachtet man vorliegend die Informationen, derer es für die Zuordnung bedarf, so befinden diese sich in der Hand desjenigen, der die Fahrer bzw. Kontrolleure beschäftigt. Für denjenigen ist die Person mithin ohne weiteres identifizierbar. Zu fragen ist jedoch, inwieweit dessen Wissen bei der Beurteilung der Identifizierbarkeit für die übrigen Teilnehmer zu berücksichtigen ist:

- *Relativer Ansatz:* Nach einem relativen Ansatz soll es nur auf die individuellen Möglichkeiten des Verantwortlichen selbst ankommen, Zusatzwissen Dritter also unbeachtlich sein.[20]
- *Absoluter Ansatz:* Nach dem absoluten Ansatz soll diese enge Betrachtung demgegenüber nicht gelten, sondern vielmehr die Möglichkeit der Identifizierung durch einen beliebigen Dritten ausreichen.[21] Einzig wenn völlig ausgeschlossen ist, dass der Verantwortliche von diesem Wissen Kenntnis erlangt, soll der Personenbezug nicht vorliegen.[22] Auf die Möglichkeit oder gar die Nutzung des Zusatzwissens abzustellen, würde den Personenbezug ins Belieben des Verantwortlichen stellen.[23] Insoweit kann zwar auf die ausdrückliche Einbeziehung von „Mitteln [...] anderer Personen" (EG 26 S. 2) verwiesen werden, diese sollen aber nur Berücksichtigung finden, wenn sie nach „allgemeinem Ermessen wahrscheinlich" (EG 26 S. 3) genutzt werden. Nicht also jedes Wissen eines Dritten reicht aus.[24]
- *Vermittelnder Ansatz:* In diesem Sinne wird zur Beurteilung des Personenbezugs vermittelnd auf die Möglichkeiten des Verantwortlichen abgestellt, dessen Wissen aber um solches Dritter ergänzt werden soll, das er sich verschaffen könnte und bei dem wahrscheinlich ist, dass er sich dieses auch verschaffen wird.[25]

14 Der EuGH hat die vermittelnde Auffassung noch zur alten Rechtslage („Mittel, das vernünftigerweise eingesetzt werden kann") aufgegriffen und die Zurechnung jedenfalls dann bejaht, wenn dem Verantwortlichen rechtliche Mittel zur Verfügung stehen, derer er sich zur Erlangung der Daten des Dritten bedienen kann.[26] Genügen soll demnach, wenn er mittelbar über eine dritte Stelle Zugriff nehmen kann, wie in jenem Fall über die Strafverfolgungsbehörde.[27] Diese Rechtsprechung ist auch auf die neue Rechtslage nach der DSGVO übertragbar.[28]

15 Entscheidend sein sollte deshalb, dem *vermittelnden Ansatz* folgend und unter Berücksichtigung der Rechtsprechung des EuGH – auch nach der DSGVO – ob der Verantwortliche insbesondere über rechtliche Möglichkeiten verfügt, an die zusätzlichen Informationen zu gelangen, und inwiefern die Nutzung dieser Möglichkeiten wahrscheinlich ist. Ein lediglich über die Kennnummer oder Standortdaten Verfügender könnte Strafanzeige (in Frage käme bei durch fehlerhafte Lebensmittel eingetretene Schäden etwa fahrlässige Körperverletzung gem. § 229 StGB, sowie Körperverletzung gem. § 223 StGB oder Sachbeschädigung gem. § 303 StGB) erstatten, sofern er etwa meint, durch das Handeln eines Kontrolleurs oder Spediteurs sei ein Schaden an der Ware entstanden oder eine Verunreinigung erfolgt, die sich nachteilig auf die Gesundheit eines Verbrauchers ausgewirkt hat. Unabhängig von einer tatsächlich strafrechtlich relevanten Handlung könnte er diese Vorgehensweise wählen, um ebenso einen zivilrechtlichen Schadensersatzanspruch durchzusetzen. Die Strafverfolgungsbehörde könnte in einem entsprechenden Ermittlungsverfahren die zusätzlichen Informationen entweder zur Identifizierung nach den §§ 94, 95 StPO beschlagnahmen, oder aber weitere Mitarbeiter nach § 161a StPO zu diesen befragen. Über das Ermittlungsverfahren erlangt so derjenige, der bisher lediglich über Standortdaten oder Kennungen verfügte, Kenntnis von den weiteren Informationen.

16 Sowohl für die Standortdaten als auch für die Qualitätskontrolldaten ist somit die rechtliche Möglichkeit gegeben, dass auch durch Zuhilfenahme Dritter der Personenbezug hergestellt werden kann. Somit liegt für die Standortdaten wie auch für die Qualitätskontrolldaten der Personenbezug nicht lediglich für den Teilnehmer, der die jeweiligen Mitarbeiter beschäftigt, sondern ebenso für jeden beliebigen, an der Blockchain beteiligten Dritten, vor.

IV. Rechtmäßigkeit der Verarbeitung

17 Soweit der sachliche Anwendungsbereich der DSGVO eröffnet ist, ist ausgehend vom Verbotsprinzip mit Erlaubnisvorbehalt die Verarbeitung von personenbezogenen Daten nur recht-

19 *Roßnagel*, ZD 2018, 243 (245).

20 *Eßer* in Auernhamer, DSGVO BDSG, 6. Aufl. 2018, Art. 4 DSGVO Rz. 20; *Buchholtz/Stentzel* in Gierschmann/Schlender/Stentzel/Veil, Art. 4 DSGVO Rz. 11; ebenfalls eher dem relativen Ansatz folgend: *Gola* in Gola, DSGVO, 2. Aufl. 2018, Art. 4 DSGVO Rz. 18.

21 *Weichert*, DuD 2007, 113 (115); *Franzen* in Franzen/Gallner/Oetker, DSGVO, 3. Aufl. 2020, Art. 4 DSGVO Nr. 1 Rz. 4.

22 *Weichert*, DuD 2007, 113 (115).

23 *Karg* in Simitis/Hornung/Spiecker, Datenschutzrecht DSGVO mit BDSG, Art. 4 DSGVO Nr. 1 Rz. 62.

24 *Klar/Kühling* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Nr. 1 Rz. 26.

25 *Arning/Rothkegel* in Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO Nr. 1 Rz. 35; *Klar/Kühling* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Nr. 1 Rz. 28.

26 EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rz. 49, CR 2016, 791 m. Anm. *Nink* – Breyer.

27 EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rz. 47, CR 2016, 791 m. Anm. *Nink* – Breyer.

28 *Klar/Kühling* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 4 DSGVO Nr. 1 Rz. 20; *Krügel*, ZD 2017, 455 (459) bejaht zwar eine Änderung durch den Wortlaut, aber nur insoweit nun auch illegale Möglichkeiten einbezogen sein sollen. Die Einschränkung auf Dritte, deren Wissen sich der Verantwortliche nutzbar machen kann, besteht auch ihr zufolge weiterhin.

mäßig, wenn eine der nach Art. 6 Abs. 1 DSGVO enumerativ aufgeführten Bedingungen erfüllt ist.

18 *Rechtliche Verpflichtung:* Soweit ein Unternehmen Daten von dem in der Versorgungskette jeweils vor- oder nachgelagerten Unternehmen speichert, um den Aufzeichnungspflichten für eine Rückverfolgbarkeit nachzukommen, folgt diese Pflicht unmittelbar aus der VO EG Nr. 178/2002 und dem LFGB, so dass eine Legitimation gem. Art. 6 Abs. 1 lit. c, Abs. 3 DSGVO in Betracht kommt. Bei EU-Verordnungen und Bundesrecht, wie vorliegend, handelt es sich um Unionsrecht bzw. Recht der Mitgliedstaaten nach Art. 6 Abs. 3 S. 1 lit. a bzw. b DSGVO.[29] Mit Blick auf das mit den Vorschriften verfolgte Ziel der Rückverfolgbarkeit zur Erreichung eines hohen Schutzniveaus der Verbraucherinteressen und Gesundheit,[30] ist die Speicherung der gesetzlich geforderten aufzuzeichnenden Daten auch verhältnismäßig. Insoweit ist die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung i.S.d. Art. 6 Abs. 1 lit. c DSGVO rechtmäßig.

19 *Erforderlichkeit für Vertragserfüllung:* Soweit Daten zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich sind, die Verarbeitung der Daten also in einem engen Sachzusammenhang zum Vertragszweck steht,[31] kann die Verarbeitung auch auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden. Für die in Rede stehenden Lieferanten- und Kundendaten gilt, dass sie ohne weiteres zur Erfüllung des Vertrages erforderlich sind, so dass eine Verarbeitung auch nach dieser Rechtmäßigkeitsbedingung zulässig wäre.

20 *Einwilligung:* Wenn jedoch weitere Unternehmen personenbezogene Daten in ihrem Blockchain-Verzeichnis ablegen und einsehen können, wenngleich sie (noch) keine Produkte von diesem Unternehmen beziehen oder an dieses liefern, so stellt dies weder eine gesetzlich geforderte, noch zur Erfüllung eines Vertrags erforderliche, Verarbeitung dar. Auch eine Verarbeitung zur Durchführung einer vorvertraglichen Maßnahme i.S.d. Art. 6 Abs. 1 lit. b DSGVO scheidet aus, da sich eine solche auf ein bestimmtes Vertragsverhältnis beziehen und die Initiative zur Verarbeitung wegen einer vorvertraglichen Maßnahme von der betroffenen Person ausgehen muss.[32] Für diese Verarbeitung bedürfte es deshalb regelmäßig einer Einwilligung der betroffenen Personen nach Art. 6 Abs. 1 lit. a DSGVO und der Erfüllung der damit verbundenen rechtlichen Anforderungen.

V. Bestimmung des Verantwortlichen

21 Der Verantwortliche ist gem. Art. 5 Abs. 2 DSGVO für die Einhaltung der in Art. 5 Abs. 1 DSGVO normierten datenschutzrechtlichen Pflichten und Grundsätze zuständig. Definiert ist der Verantwortliche in Art. 4 Nr. 7 DSGVO als diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Anders als bei einer klassischen Datenbank fehlt in einer Blockchain, also einem verteilten Netzwerk, eine zentrale Instanz, die über die Verarbeitung entscheidet. Stattdessen ist eine Vielzahl von Stellen beteiligt, die sowohl Daten einbringen, als auch speichern und damit verarbeiten. Fraglich ist deshalb, welcher der Beteiligten innerhalb der Blockchain als Verantwortlicher zu qualifizieren ist.

1. Absender

Allgemein wird angenommen, dass jedenfalls derjenige Teilnehmer, der eine Information absendet, Verantwortlicher ist.[33] 22
Dies ist folgerichtig, da ihm die Entscheidung obliegt, ob, warum und wofür ein Datum verarbeitet wird. Damit entscheidet er über die Zwecke und, indem er sich des der Blockchain zugrunde liegenden Algorithmus bedient, über die Mittel der Verarbeitung.

2. Gemeinsame Verantwortlichkeit

An einem Blockchain-Netzwerk und den einzelnen Verarbeitungsvorgängen sind zumeist mehrere Personen beteiligt. Neben demjenigen, der eine Information einbringt, müssen zunächst weitere Teilnehmer die Information verarbeiten. Erst anschließend wird sie den Verzeichnissen der Blockchain hinzugefügt. Wegen der Vielzahl der Beteiligten könnte deshalb auch eine gemeinsame Verantwortlichkeit (sog. „joint controllership", Art. 26 DSGVO) angenommen werden. Eine solche wird aber zum Teil mit dem Hinweis auf regelmäßig fehlende Absprachen und mangelnden Einfluss auf die Verarbeitung anderer Beteiligter in der Blockchain grundsätzlich abgelehnt.[34] Nur soweit ausnahmsweise „gezielte, gemeinsam[e] Entscheidungen über die Verwendung der Blockchain zu einem konkreten Datenverarbeitungszweck" getroffen werden, soll dies eine gemeinsame Verantwortlichkeit zur Folge haben. 23

Auch wird argumentiert, dass die bloße „Mitursächlichkeit für einen Datenstrom" nicht genüge, und es demgegenüber einer gemeinsamen Festlegung des Ziels und der hierzu eingesetzten Mittel bedürfe. In Ermangelung dessen fehle es demnach bei den Teilnehmern einer Blockchain regelmäßig an einer gemeinsamen Verantwortlichkeit.[35] Dagegen wird angeführt, dass nicht ein einzelner Teilnehmer über die Verarbeitung entscheide, sondern jeder Teilnehmer zu gleichen Teilen an der Verarbeitung der Daten beteiligt sei, weshalb grundsätzlich die gemeinsame Verantwortlichkeit aller Beteiligten anzunehmen sei.[36] Infolge des Wortlauts des Art. 26 Abs. 1 S. 1 DSGVO, der eine gemeinsame Zweck- und Mittelfestlegung zur Annahme der gemeinsamen Verantwortlichkeit verlangt, ist schon aus rein praktischen Gründen der Auffassung zuzustimmen, dass nicht jede Form der Hilfeleistung der anderen Beteiligten bei der Verarbeitung die Annahme einer gemeinsamen Verantwortlichkeit begründen kann. 24

Verglichen mit anderen Anwendungsfällen grenzt sich die vorliegend für den Lebensmittelsektor zu betrachtende Umsetzung 25

29 Vgl. *Frenzel* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rz. 35 f.
30 Siehe: Art. 1 Abs. 1 S. 1 VO EG Nr. 178/2002; § 1 Abs. 1 Nr. 1 LFGB.
31 *Spindler/Dalby* in Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DSGVO Rz. 6.
32 Siehe zu der erforderlichen Nähe zu einem bestimmten Vertragsverhältnis und der Initiative der betroffenen Person *Frenzel* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rz. 15.
33 *Janicki/Saive*, ZD 2019, 251 (254).
34 *Janicki/Saive*, ZD 2019, 251 (254).
35 *Martini* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 26 DSGVO Rz. 19 ff.
36 *Bechtolf/Vogt*, ZD 2018, 66 (69).

der Blockchain insbesondere dadurch ab, dass sich die Teilnehmer der Anwendung nicht bloß zur Durchsetzung einzelner, isolierter Individualinteressen bedienen. Die Verarbeitung dient vorliegend vielmehr dem gemeinsamen Zweck der Absicherung der gesamten Versorgungskette. Hierzu bedienen sich die Beteiligten des Netzwerks, indem sie selbst Daten einbringen, aber auch indem sie solche der anderen Teilnehmer weiterverarbeiten. Die Bestimmung hinsichtlich der Zwecke der Verarbeitung erfolgt durch Beitritt deshalb zumindest konkludent.[37] Wegen den qualifizierten gemeinsamen Zwecken, zu deren Erreichung sich die Teilnehmer der Blockchain bedienen, begründet das Zusammenwirken eine gemeinsame Verantwortlichkeit. Damit auch unter diesen Bedingungen die Betroffenenrechte erfüllt werden können, haben die Verantwortlichen in einer transparenten Vereinbarung ihre jeweiligen Verantwortlichkeiten zu regeln.[38]

VI. Löschung

26 Eine wesentliche Eigenschaft der Blockchain-Technologie ist die Unveränderbarkeit der einmal eingebrachten Daten. Diese Unveränderbarkeit konfligiert mit wesentlichen Grundsätzen des Datenschutzrechts, wonach die Speicherung personenbezogener Daten gem. Art. 5 Abs. 1 lit. c DSGVO auf ein notwendiges Minimum zu beschränken ist. Nicht (mehr) benötigte Daten sind deshalb zu löschen. Darauf, dass die sie betreffenden personenbezogenen Daten unverzüglich, also ohne unangemessene Verzögerung,[39] gelöscht werden, hat die betroffene Person insb. gem. Art. 17 Abs. 1 lit. a DSGVO dann ein Recht, wenn die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Ein Recht auf Löschung der Daten besteht ebenso gem. Art. 17 Abs. 1 lit. b DSGVO, wenn die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt. Die datenschutzrechtlich verstandene Löschung meint die Unkenntlichmachung von Daten in einer Weise, dass sie für den Verantwortlichen unlesbar sind.[40] Für die Blockchain-Technologie werden deshalb verschiedene Ansätze in Bezug auf die Umsetzung einer so verstandenen Löschung diskutiert.

1. (Unbegrenzte) Rechtmäßigkeit der Verarbeitung

27 Ein vorgeschlagener Ansatz besteht darin, die verlangte Löschung zu versagen.[41] Dies soll möglich sein, soweit „die Existenz der gesamten Blockchain gefährdet“[42] würde und deshalb eine vorzunehmende Interessenabwägung zugunsten der verantwortlichen Betreiber ausfalle. In die Interessenabwägung seien insoweit das aus Art. 7 und 8 GR-Charta folgende „Recht auf Vergessenwerden“ einerseits und andererseits jenes aus Art. 16 GR-Charta auf unternehmerische Freiheit einzustellen, wobei Letzteres durchaus überwiegen könne.[43]

28 Eine solche Interessenabwägung ist zunächst dann eröffnet, wenn einer der – hier grundsätzlich nicht einschlägigen – Fälle des Art. 17 Abs. 3 DSGVO vorliegt.[44] Außerdem, wenn das Löschungsverlangen auf dem Widerruf der Einwilligung fußt und die Verarbeitung stattdessen theoretisch auf Art. 6 Abs. 1 lit. f DSGVO als andere Rechtmäßigkeitsbedingung gestützt werden könnte,[45] die eine Interessenabwägung voraussetzt. Oder schließlich, wenn die Verarbeitung dem Grunde nach auf einer gesetzlichen Verpflichtung beruht bzw. zur Vertragserfüllung erforderlich ist, für die (zeitlich) darüberhinausgehende Speicherung von Vornherein aber ausschließlich Art. 6 Abs. 1 lit. f DSGVO als Rechtmäßigkeitsbedingung in Frage kommt.

29 Falls die Datenverarbeitung in der Blockchain (auch) auf eine Interessenabwägung gem. Art. 6 Abs. 1 lit. f DSGVO gestützt werden soll, so müsste sie im berechtigten Interesse des Verantwortlichen liegen und die Interessen der betroffenen Person dürften nicht überwiegen. Das berechtigte Interesse für die Datenverarbeitung ist grundsätzlich weit zu fassen.[46] Dieser weiten Auslegung wird im Rahmen der Interessenabwägung mit dem einschränkenden Kriterium der Erforderlichkeit begegnet. Hierbei trifft die betroffene Person die Darlegungslast, dass ihre Interessen überwiegen.[47] Abzuwägen ist anhand des Einzelfalls unter Berücksichtigung der konkreten Umstände. Hierbei ist zugunsten der betroffenen Person zunächst zu berücksichtigen, ob die konkrete Form der Datenverarbeitung für sie zuvor erkennbar gewesen ist. Des Weiteren ist in die Interessenabwägung die Schwere des Eingriffs in ihre Rechte einzustellen, wobei es maßgeblich auf die Art der verarbeiteten Daten ankommen dürfte. Für Daten der einzelnen, an der Lieferkette beteiligten Unternehmen, die etwa auf deren jeweiligem Internetauftritt oder in öffentlichen Registern einsehbar sind, ist die Schwere des Eingriffs eher als gering einzustufen. Die potentiell unbegrenzte Dauer der Speicherung hingegen ist, da sie das Recht auf Löschung in Frage stellt, erschwerend zu berücksichtigen. Es muss deshalb ein überragendes Interesse bestehen, das die Umsetzung der Datenverarbeitung in dieser Form zwingend erforderlich macht. Bestehen – zumindest im Rahmen der Gestaltung und Umsetzung des konkreten technischen Ansatzes im Sinne von Privacy by Design – mildere Mittel, so sind diese zur Wahrung der beiderseitigen Interessen vorzugswürdig und dürften die Abwägung zu Lasten des Verantwortlichen ausfallen lassen.

30 Allenfalls für wenige – öffentlich einsehbare – Daten könnte damit überhaupt die Abwägung zugunsten des Verantwortlichen ausfallen. Angesichts der im Folgenden dargestellten milderen Mittel ist aber selbst für diese Daten ein Überwiegen der Interessen wohl in aller Regel nicht anzunehmen. Zu be-

37 Hinsichtlich der Verantwortlichkeit wird nur auf den faktischen Einfluss, und nicht eine formale Bezeichnung geachtet, s. *Martini* in Paal/Pauly, DSGVO BDSG, 2. Aufl. 2018, Art. 26 DSGVO Rz. 20.

38 *Spoerr* in BeckOK Datenschutzrecht, DSGVO, 29. Ed. 1.8.2019, Art. 26 DSGVO Rz. 32, 34.

39 *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, Art. 17 DSGVO Rz. 10.

40 *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, Art. 17 DSGVO Rz. 10.

41 https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf S. 33 (3.1.2020).

42 https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf S. 33 (3.1.2020).

43 https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf S. 33 (3.1.2020).

44 Zur Interessenabwägung in diesen Fällen vgl. *Kamann/Braun* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 17 DSGVO Rz. 55.

45 Siehe zur Möglichkeit, die Verarbeitung im Falle des Widerrufs der Einwilligung auf berechtigte Interessen zu stützen *Veil*, NJW 2018, 3337 (3342).

46 *Albers/Veit* in BeckOK Datenschutzrecht, DSGVO, 29. Ed. 1.8.2019, Art. 6 DSGVO Rz. 49 ff.

47 Sobald die betroffene Person anschließend der Verarbeitung widerspricht, kehrt sich jedoch die Darlegungslast um: *Albers/Veit* in BeckOK Datenschutzrecht, DSGVO, 29. Ed. 1.8.2019, Art. 6 DSGVO Rz. 52.

achten ist auch, dass sofern für einzelne oder alle Daten – etwa durch ein Gericht – ein überwiegendes Interesse des Verantwortlichen verneint wird, nach diesem Ansatz eine Löschung von Daten bei gleichzeitigem Erhalt der Blockchain ausgeschlossen ist.

2. Verschlüsselung

31 Als weitere Möglichkeit einer datenschutzrechtlich verstandenen Löschung käme in Betracht, die personenbezogenen Daten innerhalb der Blockchain nur verschlüsselt abzulegen und den notwendigen Entschlüsselungskey außerhalb der Blockchain, also „off-chain", zu speichern.[48] Eine Löschung der personenbezogenen Daten könnte dann so gesehen schon durch die Vernichtung des Entschlüsselungskeys erfolgen, denn vergleichbar mit der Unlesbarkeit eines auf Papier gedruckten, aber übermalten und damit den Anforderungen der Löschung genügenden Datums,[49] genügt auch hier die Unlesbarkeit. Die Herstellung eines Personenbezugs müsste jedoch den Kriterien in ErwGr 26 S. 4 zur DSGVO entsprechend ausgeschlossen sein. Es müsste folglich eine Unumkehrbarkeit gewährleistet werden, die Verschlüsselung also *entschlüsselungssicher* sein. Ausdrücklich sind demzufolge sowohl bereits verfügbare Technologien, aber ebenso zu erwartende technologische Entwicklungen zu berücksichtigen. Die Verschlüsselung muss damit vor einer Entschlüsselung durch auch zukünftige[50] Technologien schützen. Diese Technologien sind i. R. einer Risikobewertung fortlaufend neu zu berücksichtigen.[51] Die Sicherheit derzeit eingesetzter Verschlüsselungen rührt daher, dass die Entschlüsselung durch herkömmliche Computer zwar möglich, jedoch äußerst langwierig und deshalb für den gängigen Gebrauch impraktikabel ist. Ob dies mit Blick auf die fortschreitende Entwicklung der Quantencomputer noch gilt, dürfte aber fraglich sein.[52]

3. Pseudonymisierung

32 Ähnlich dem vorstehend dargestellten Ansatz ist eine weitere „off-chain"-Lösung denkbar: Ordnet man Daten in der Blockchain anstelle Namen lediglich Pseudonymen zu, und die Pseudonyme lediglich „off-chain" den Namen, kann statt der Löschung der Daten die Vernichtung der „off-chain" gespeicherten Zuordnungen erfolgen.[53] Die in der Blockchain gespeicherten Daten sind anschließend zwar nicht aus der Blockchain entfernt, jedoch lediglich noch einem Pseudonym zuordenbar, das seinerseits aber keine Zuordnung zu einer bestimmten Person erlaubt. Die Daten sind damit dem Grunde nach nicht länger personenbezogen. Zu berücksichtigen sind jedoch auch hier (zukünftige) Technologien, die dazu genutzt werden können, aus der Vielzahl einem bestimmten Pseudonym zugeordneter Daten die dahinterstehende Person zu ermitteln.[54] Weiter ist auch zu beachten, dass u.U. zwar einzelne Datensätze gelöscht werden sollen bzw. deren Personenbezug entfallen soll, gleichzeitig aber andere, dem gleichen Pseudonym zugeordnete Datensätze, weiterhin zuordenbar bleiben sollen. Um diese teilweise Zuordnung zu ermöglichen und zugleich die Bestimmung einer Person mittels Auswertung einer Vielzahl einem Pseudonym zugeordneter Datensätze zu verhindern, empfiehlt sich in der Praxis deshalb die regelmäßige Neuvergabe eines Pseudonyms (vergleichbar mit dynamischen IP-Adressen).

VII. Fazit

Trotz Personenbezogenheit der zur Absicherung von Versor- 33
gungsketten im Lebensmittelsektor zu speichernden Daten ist eine datenschutzkonforme Gestaltung der Blockchain nicht ausgeschlossen. Dies gilt insbesondere mit Blick auf das Recht auf Löschung. Zur Vermeidung von Rechtsunsicherheit sollte die Datenschutzkonformität jedoch nicht von einer zugunsten des Verantwortlichen ausfallenden Interessenabwägung abhängen. Darüber hinaus ist durch *Privacy by Design* schon bei der Entwicklung neuer Blockchain-Technologien sicherzustellen, dass die eingebrachten personenbezogenen Daten auf ein notwendiges Minimum beschränkt werden und dieses Minimum seinerseits vorzugsweise nur verschlüsselt und referenziert abgelegt wird. Dabei ist stets die fortschreitende Entwicklung des *Standes der Technik* zu berücksichtigen, die ggf. Anpassungen erfordert. Der gemeinsamen Verantwortlichkeit der an der Blockchain Beteiligten ist durch eine entsprechende Vereinbarung Rechnung zu tragen, um der betroffenen Person eine effektive Ausübung ihrer Rechte zu ermöglichen und die datenschutzrechtlichen Zuständigkeiten auch innerhalb eines vernetzten Systems eindeutig zu bestimmen.

Dr. Dennis-Kenji Kipker

Wissenschaftlicher Geschäftsführer am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

IT-Sicherheitsrecht, Datenschutzrecht

kipker@uni-bremen.de

https://denniskenjikipker.de/

Hauke Bruns

Studentischer Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

brunsh@uni-bremen.de

48 Siehe auch: BSI, Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen, März 2019, S. 63.

49 *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, Art. 17 DSGVO Rz. 10.

50 *Spindler/Dalby* in Spindler/Schuster Recht der elektronischen Medien, DSGVO, 4. Aufl. 2019, Art. 4 DSGVO Nr. 1 Rz. 9.

51 *Klabunde* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 4 DSGVO Rz. 17.

52 Zu den Gefahren für derzeit eingesetzte Verschlüsselungsverfahren durch Quantencomputing: Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung (HMWEVL), Quantencomputer und „Next Generation Crypto", S. 1 f.; zu stattdessen einsetzbarer „Post-Quantum-Kryptografie" s.: *ebd.* S. 8.

53 Siehe auch: *Martini/Weinzierl*, NVwZ 2017, 1251 (1256).

54 *Martini/Weinzierl*, NVwZ 2017, 1251 (1256) halten die Herstellung des Personenbezugs via Big Data für möglich.