(GEG) geregelt.[39] Da dem für die Bauaufsicht zuständigen Ministerium bekannt war, dass die Gesetzesvorlage im Bundestag in dritter Lesung bereits am 18. 6. 2020 beschlossen wurde und nur noch die Zustimmung des Bundesrates ausstand, hätte sie in dem am 22. 7. 2020 dem Landtag Brandenburg zugeleiteten Gesetzentwurf, Dr 7/1697, eine Änderung des Verweises des § 4 S. 2 BbgBO auf das GEG aufnehmen müssen. Spätestens nach der Verkündung des GEG am 13. 8. 2020 im Bundesgesetzblatt hätte die Änderung des § 4 S. 2 in das laufende Gesetzgebungsverfahren eingebracht werden müssen, da mit der Verkündung bekannt war, dass das GEG am 1. 11. 2020 in Kraft tritt und die Energieeinsparverordnung gleichzeitig außer Kraft tritt.

II. Zusammenfassung

Die aufgezeigten Beispiele belegen, dass die BbgBO dringend einer weiteren Novelle bedarf. Dabei sollten die inhaltlichen Mängel und die sprachlichen Fehler beseitigt werden. Ferner bedarf die BbgBO wohl einer eingehenden Prüfung auf ihre Rechtsförmlichkeit nach dem Handbuch der Rechtsförmlichkeit.[40] Der Landesgesetzgeber sollte auch prüfen, ob die Eingriffe in die freie Berufsausübung der Fachplaner gerechtfertigt sind. Insgesamt bedarf auch die Musterbauordnung einer sprachlichen Überarbeitung und einer Rechtsförmlichkeitsprüfung. Die Fachkommission Bauaufsicht sollte sich damit befassen, ob sich der Anwendungsbereich der Musterbauordnung strikt an dem Anwendungsbereich der Bauproduktenverordnung orientieren muss.

Die bisherige Auslegung des § 2 I 1 MBO, wonach auch Verkaufsfahrzeuge oder Boote, die überwiegende ortsfest genutzt werden, bauliche Anlagen sind, dürfte mit der durch Bauproduktenverordnung vorgegebenen Definition der Bauprodukte nicht vereinbar sein. Die bisherige Auslegung machte die Bauaufsichtsbehörden für naturschutzrechtliche oder wasserrechtliche Probleme verantwortlich, die eigentlich in die Zuständigkeit der Naturschutzbehörden fallen und von diesen unter Berücksichtigung auch der §§ 29 ff und insbesondere des § 36 I 2 BauGB selbst entschieden werden können.

39 Das Gebäudeenergiegesetz wurde als Art. 1 des Gesetzes zur Vereinheitlichung des Energieeinsparrechts für Gebäude mit der Dr 19/16716 durch die Bunderegierung am 22. 1. 2020 in den Bundestag eingebracht. Das Gesetz zur Vereinheitlichung des Energieeinsparrechts für Gebäude und zur Änderung weiterer Gesetze wurde in Dritter Lesung am 18. 6. 2020 vom Bundestag beschlossen. Als Datum des Inkrafttretens war der erste Tag des dritten auf die Verkündung folgenden Monat vorgesehen. Der Bundestag hat das Gesetz am 18. 6. 2020 verabschiedet. Der Bundesrat hat das GEG am 3. 7. 2020 durch Beschluss bestätigt. Damit war vor der Einbringung der Drucksache 7/7/1697 in den Landtag Brandenburg am 22. 7. 2020 klar, dass eine Änderung des Verweises in § 4 S. 2 BbgBO erforderlich wurde. Das Gesetz zur Vereinheitlichung des Energieeinsparrechts für Gebäude und zur Änderung weiterer Gesetze am 13. 8. 2020 im BGBL. I Nr. 63 verkündet und ist am 1. 11. 2020 in Kraft getreten. Gleichzeitig ist die die Energieeinsparverordnung außer Kraft getreten.

40 Bekanntmachung des Handbuchs der Rechtsförmlichkeit vom 22. 9. 2008, Bundesanzeiger 2008 Nr. 160 a.

Die behördliche Kontrolle durch Blockchain-Technologie in der Agrar- und Ernährungswirtschaft – Datenschutzrechtliche Anforderungen

Philipp Schöbel, Frankfurt (Oder)*

Der Einsatz von Blockchain-Technologie ermöglicht eine Transparenz von Liefer- und Wertschöpfungsketten in einem Maß, dass die Rechtsdurchsetzung und den Verbraucherschutz enorm verbessern kann. Das macht deren Einsatz für die jeweils für die Lebensmittelüberwachung zuständigen Behörden attraktiv. Dabei ist die Frage der Vereinbarkeit mit dem europäischen Datenschutzrecht von der konkreten Anwendung der Technologie abhängig.

I. Einleitung

Innovationen im Agrarsektor sind erforderlich, um die immensen Herausforderungen der Ernährung der Weltbevölkerung, wie Klimawandel, Dürren, Überschwemmungen, Desertifikationen, den Verlust der Artenvielfalt, Schädlinge und Krankheiten zu bewältigen.[1] Die überwiegende Zahl der deutschen Landwirte sieht in digitalen Technologien eine Möglichkeit um ressourcenschonend, umweltfreundlich und nachhaltig zu produzieren.[2] Auch die Blockchain-Technologie schafft neue Möglichkeiten für eine nachhaltige Landwirtschaft 4.0.[3] Die Technologie bietet zudem ein enormes Potential was die Sichtbarmachung einzelner Schritte in Wertschöp-

* Der Autor ist Akademischer Mitarbeiter am Lehrstuhl für Öffentliches Recht, Verwaltungs-, Europa-, Umwelt-, Agrar- und Ernährungswirtschaftsrecht | Forschungsstelle für Digitalrecht | (Prof. *Dr. Ines Härtel*, Richterin des Bundesverfassungsgerichts) an der Europa-Universität Viadrina, Frankfurt (Oder). - Der Beitrag ist im Rahmen des BMBF-Verbundprojekts DAKIS entstanden, s. https://www.agrarsysteme-der-zukunft.de/konsortien/dakis

1 E-Agriculture in Action: Blockchain – For Agriculture – Opportunities and Challanges, Sylvester (edt.), publ. By the Food and Agriculture Organization of the United Nations and International Telecommunication Union, 2019, S. V; *Härtel*, NuR 2020, 439 f.; *dies.*, Wege der Ernährungswirtschaft – global, regional, europäisch, 2017, S. 13 (18 ff.).

2 DBV, Pressemitteilung, Schon 8 von 10 Landwirten setzen auf digitale Technologien, vom 27. 4. 2020, abrufbar unter https://www.bauernverband.de/presse-medien/pressemitteilungen/pressemitteilung/schon-8-von-10-landwirten-setzen-auf-digitale-technologien.

3 So bereits *Härtel*, NuR 2019, 577 (578).

fungsketten betrifft. Aus dem Blickwinkel der Lebensmittelsicherheit schafft dies neue Möglichkeiten von Überwachung und Informationsgewinnung.

1. Begriff Blockchain

Um die rechtlichen und politischen Aspekte der Blockchain zu bewerten, ist ein grundlegendes technisches Verständnis der Technologie erforderlich. Die Blockchain-Technologie ermöglicht den Transfer von Informationen in einem dezentral verwalteten Register.[4] Für das Konzept der Blockchain sind die fünf Wesensmerkmale Daten-Integrität, Daten-Ubiquität, Datenunveränderbarkeit, Datensicherheit und kryptografische Identität charakterisierend.[5]

Die Blockchain funktioniert als eine Art dezentrale Datenbank.[6] Informationen werden in aneinandergereihten Datenblöcken chronologisch gespeichert und mittels eines digitalen Fingerabdrucks (sogenannte Hashes) miteinander verkettet.[7] Dabei hat jeder Block seinen eigenen Hash und einen Hinweis auf den Hash des vorherigen Blocks.[8] Die einzelnen Blöcke sind mit den Seiten eines Registerbuchs vergleichbar.[9] Dabei werden auf jedem an dem Netzwerk beteiligten Rechner alle Daten der Kette gespeichert, was zu einer maximalen Transparenz führen soll.[10] Das Hinzufügen eines neuen Blocks bedarf dabei der Genehmigung durch das Netzwerk,[11] wobei bei der klassischen Ausgestaltung der Technologie eine vorher definierte Mehrheit anderer Teilnehmer (sogenannte „nodes") den neuen Datenblock bestätigen muss.[12] Dieses dezentrale Konsensverfahren bietet ein hohes Maß an Manipulationssicherheit.[13] Diese technischen Eigenschaften führen dazu, dass keine Intermediäre (z.B. Banken) für den Transfer benötigt werden.[14] Da die Speichereinträge aufeinander aufbauen, wird die Blockchain weitestgehend unveränderlich.[15] Deshalb sind Blockchain-Transaktionen transparent, kryptografisch gesichert, für immer gespeichert, nicht manipulierbar, zeitlich nachvollziehbar und dezentral validiert.[16] Durch das stetige Wachsen der Kette steigt mit jeder Transaktion der Rechenaufwand und damit auch sowohl Energiekosten als auch Zeitaufwand.[17]

Es werden grundlegend drei verschiedene Formen der Blockchain unterschieden: die private Blockchain, die öffentliche Blockchain und die Konsortium-Blockchain.[18] Die Konsortium-Blockchain wird durch eine Gruppe von Teilnehmer kontrolliert und der Prozess der Überprüfung und des Hinzufügens von Blöcken durch einen Zustimmungsmechanismus festgelegt.[19] Bei der privaten Blockchain wird der Zugang durch eine zentrale Instanz geregelt, so dass nur Personen mit einer bestimmten Echtheitsprüfung und Erlaubnis Teil des Netzwerks sein können und daher auch nur diese Daten hinzufügen und verifizieren können – wobei die Blockchain aber auch nach außen hin einsehbar sein kann.[20] Bei der öffentlichen Blockchain gibt es keine Zugangsbeschränkung und allen Personen ist das Hinzufügen und Überprüfen von Daten grundsätzlich möglich.[21]

2. Rückverfolgbarkeit bei Agrarerzeugnissen und verarbeiteten Lebensmitteln zur Gewährleistung der Lebensmittelsicherheit und Lebensmittelqualität

Die Rückverfolgbarkeit von Lebensmitteln ist ein wichtiges Instrument der Gefahrenabwehr und Vorsorge.[22] Ein Anwendungsbereich der Blockchain-Technologie besteht in genau diesem Bereich, dazu kann mittels der Blockchain die Produktions-/Lieferkette nachverfolgt werden.[23] Vorteilhaft ist hier die Einsehbarkeit der Daten durch die Beteiligten und der Ausschluss einer nachträglichen Änderung der Daten.[24] Zudem können auch Standort-Daten erfasst werden, was das Verfolgen der Transportwege ermöglichen würde.[25] So ist z.B. die Nachverfolgbarkeit der Kühlkette durch den Einsatz von Blockchain-Technologie möglich.[26] Die Anwendung der Technologie kann eine Vielzahl von Zielen verfolgen; z.B.: Erhöhung der Lebensmittelsicherheit, Effizienz der Lieferketten und Abwicklungsprozesse, Frische der Lebensmittel, Allgemeine Verbesserung der Nachhaltigkeit, Markenvertrauen, Reduktion von Lebensmittelverschwendung, Vermeidung von Lebensmittel- und Markenfälschungen.[27] Für den Fall eines Seuchenausbruchs können befallene tierische oder pflanzliche Produkte schneller zurückverfolgt werden.[28] Im Bereich des Lebensmittelhandels kann durch den Einsatz der Technologie die ganze Wertschöpfungskette (Saatguthersteller > Farm / Düngung / Ernte > Genossenschaft / Verarbeiter > Transport, Kühlkette, Import / Export > Lebensmittelherstellung & -verarbeitung > Groß-, Zwischen- & Einzelhandel > Kunde, Ver-

4 *Bechtolf/Vogt*, ZD 2018, 66 (67).
5 *Bechtolf/Vogt*, ZD 2018, 66 (67).
6 *Omlor*, ZRP 2018, 85 (86); *Hoffer/Mirtchev*, NZKart 2019, 239 (239); *Paulus*, JuS 2019, 1049 (1049).
7 *Martini/Weinzierl*, NVwZ 2017, 1251 (1251).
8 *Sylvester* (o.Fußn. 1), S. 2.
9 *Janicki/Saive*, ZD 2019, 251 (251).
10 *Schrey/Thalhofer*, NJW 2017, 1431 (1432).
11 *Weiss*, JuS 2019, 1050 (1051).
12 *Schäfer/Eckhold,* in: *Assmann/Schütze/Buck-Heeb*, Handbuch des Kapitalanlagerechts, 5. Aufl. (2020), § 16 a Crowdfunding, Crowdlending, Crowdinvesting, Kryptowährungen und Initial Coin Offerings (ICOs), Rn. 25.
13 *Simmchen*, MMR 2017, 162 (163).
14 *Ebd.,* S. 162.
15 *Hoffer/Mirtchev*, NZKart 2019, 239 (240).
16 *Schrey/Thalhofer*, NJW 2017, 1431 (1433).
17 *Paulus*, JuS 2019, 1049, (1050).
18 *Sylvester* (o.Fußn. 1), S. 3.
19 *Sylvester* (o.Fußn. 1), S. 3.
20 Zur Rückverfolgbarkeit im Bereich der Lebensmittelsicherheit vgl. u.a. *Härtel/Yu*, Food Security and Food Safety, in: *Härtel* (ed.), Handbook of Agri-Food Law in China, Germany, European Union, 2018, S. 57 (76 ff.) *Sylvester* (o.Fußn. 1), S. 3.
21 *Sylvester* (o.Fußn. 1), S. 4.
22 *Scherzberg/Garbe*, ZLR 2018, 198 (214).
23 *Kipker/Bruns*, CR 2020, 210 (210).
24 *Kipker/Bruns*, CR 2020, 210 (211).
25 *Kipker/Bruns*, CR 2020, 210 (212).
26 DLG-Expertenwissen 6/2019, Blockchain in der Food Supply Chain – Grundlagen, Praxisbeispiele, Perspektiven, S. 7; *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 9.
27 S. 8. DLG-Expertenwissen 6/2019, Blockchain in der Food Supply Chain – Grundlagen, Praxisbeispiele, Perspektiven, S. 8.
28 *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 19.

braucher) abgebildet werden.[29] Saatguthersteller können Informationen über Getreide, verwendete Pestizide, Düngemittel bereitstellen und Transaktionen mit Landwirten in einer Blockchain hinterlegen. Landwirte würden dann Informationen über die Anbaumethoden, die Wetterverhältnisse oder das Wohlergehen von Nutztieren hinterlegen. Informationen über die Verarbeitung, wie die verwendeten Geräte, Verarbeitungsmethoden und die Chargennummern könnten gespeichert werden. Im Transportbetrieb würden Informationen über Lagerverhältnisse (z.B. Feuchtigkeit, Temperatur), Transportwege, Lieferzeiten und Transportmethoden in der Blockchain gespeichert werden. Im Einzelhandel würden schließlich Informationen über einzelne Lebensmittel, deren Qualität und Quantität, ihre Verfallsdaten, die Lagerverhältnisse und die Zeit, die sie im Regal lagern, abgespeichert. Am Ende könnten Konsumenten z.B. per QR-Code Informationen über die Produkte abrufen.[30] Die Blockchain-Technologie wird in der Lieferkette von Unternehmen im Lebensmittelsektor schon für unterschiedliche Produkte, wie z.B. Hühner, Bier, Weintrauben und Thunfisch eingesetzt.[31] Der Einsatz der Technologie kann daher im Umgang mit Lebensmitteln ein neues Maß an Transparenz schaffen. Transparenz kann wiederum das Vertrauen der Verbraucher in die Lebensmittelkette stärken.[32] Der Einsatz der Technologie könnte deshalb das Vertrauen der Verbraucher in das jeweilige Endprodukt steigern.

Die Einsichtnahme in sämtliche Unterlagen der Lebensmittelproduzenten ist Teil der behördlichen Überwachungsbefugnisse.[33] Die schnellere Rückverfolgbarkeit in der Wertschöpfungskette beseitigt etwaige Unsicherheiten in der Entscheidungsfindung der Behörden. Die Transparenz der einzelnen Produktionsschritte macht etwaige Fehler- und Gefahrenquellen schneller sichtbar und ermöglicht dadurch ein schnelleres Handeln der Behörden. Für amtliche Wahrnehmungen vor dem Verzehr von Lebensmitteln bedeutet dies, dass die Ermittlung eines hinreichenden Verdachts eines Gesundheitsrisikos (Art. 10 Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (Lebensmittel-Basisverordnung), § 40 Lebensmittel-, Bedarfsgegenstände- und Futtermittelgesetzbuch (LFGB))[34] wesentlich erleichtert wird. Somit stärkt der Einsatz von Blockchain-Technologie die Rechtsdurchsetzung und führt damit zu einem erhöhten Gesundheitsschutz der Verbraucher.

II. Praktische Probleme bei der Anwendung von Blockchain

Dem flächendeckenden Einsatz der Blockchain-Technologie stehen in der Praxis einige Hürden im Weg. Durch den mit jedem zusätzlichen Block steigenden Energieverbrauch kann eine Blockchain (ab einer bestimmten Länge) ökologisch und/oder ökonomisch mehr Schaden als Nutzen bringen. Deutsche Landwirte sehen in der Praxis vor allem einen Mangel an Mitarbeitern mit dem entsprechenden Know-how, Gefahren durch potenzielle Hackerangriffe und hohe Investitionskosten als Probleme an.[35] Die Verbindung von einer Blockchain-Anwendung und anderer Software oder manueller Aufzeichnungen (oracles) wird meist von Intermediären gesteuert und kann damit das durch Dezentralisierung aufgebaute Vertrauen schwächen.[36] Die zur Teilnahme an einem durch Blockchain gesteuerten Warenhandel erforderlichen Ressourcen könnten zudem neue Produzenten oder Abnehmer abschrecken.[37] Problematisch ist auch, dass je nach Ausgestaltung und Beschaffenheit der Blockchain, eine Transaktion mehrere Minuten bis zu Stunden dauern kann,[38] was gerade bei zeitsensiblen Sachverhalten gegen den Einsatz der Technologie spricht. Zudem stellen auch im Bereich Blockchain fehlende oder schlechte Internetverbindungen ein Problem dar.[39] Ein flächendeckender Breitbandausbau im ländlichen Raum würde der Agrarindustrie 4.0 zugutekommen. So fordert auch eine deutliche Mehrheit der deutschen Landwirte einen besseren Breitband- und Mobilfunkausbau.[40]

III. Datenschutzrechtliche Anforderungen an den Einsatz von Blockchain

Der Einsatz der Technologie muss mit der Datenschutzgrundverordnung (DSGVO) vereinbar sein.

1. Sachlicher Anwendungsbereich der DSGVO

Der Anwendungsbereich der DSGVO ist sachlich eröffnet, soweit es um die Verarbeitung personenbezogener Daten geht (Art. 2 I DSGVO). Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4. I DSGVO).[41] In der deutschen Landwirtschaft dominieren Einzelunternehmen mit

29 DLG-Expertenwissen 6/2019, Blockchain in der Food Supply Chain – Grundlagen, Praxisbeispiele, Perspektiven, S. 9.

30 *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 6 f.

31 Eine Vielzahl von Beispielen auflistend: *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 9 ff.

32 *de Boer*, Transparency and consumer trust in scientific assessments under European food law, in: The functional field of food law, *Urazbaeva/Szajkowska*, 245 (253).

33 *Riemer* in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 58. Compliance in der Lebensmittelwirtschaft, 3. Aufl. (2016), Rn. 99.

34 Zum Begriff des hinreichenden Verdachts eines Gesundheitsrisikos siehe im Einzelnen *Pache/Meyer in: Meyer/Streinz*, LFGB – BasisVO, 2. Aufl. (2012), Rn. 19 ff.

35 Zu einer repräsentativen Umfrage: DBV, Pressemitteilung, Schon 8 von 10 Landwirten setzen auf digitale Technologien, vom 27.4.2020, abrufbar unter https://www.bauernverband.de/presse-medien/pressemitteilungen/pressemitteilung/schon-8-von-10-landwirten-setzen-auf-digitale-technologien.

36 *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 22.

37 *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 22.

38 *Kamilaris/Fonts/Prenafeta-Boldú*, The Rise of Blockchain Technology in Agriculture and Food Supply Chains, S. 24.

39 *Sylvester* (o.Fußn. 9), S. 30.

40 So DBV, Pressemitteilung, Schon 8 von 10 Landwirten setzen auf digitale Technologien, vom 27. 4. 2020, abrufbar unter https://www.bauernverband.de/presse-medien/pressemitteilungen/pressemitteilung/schon-8-von-10-landwirten-setzen-auf-digitale-technologien.

41 Zur DSGVO mit Blick auf die Landwirtschaft 4.0 vgl. *Härtel*, NuR 2019, 577 (583 f.); dies., NuR 2020, 439 (444 ff.).

einem Anteil von 89 Prozent.[42] Für einen Großteil der deutschen Urproduktion besteht deshalb ein Personenbezug, weswegen der Anwendungsbereich der DSGVO eröffnet ist.[43]

Der *EuGH* hat entschieden, dass Daten über juristische Personen dann als Daten natürlicher Personen angesehene werden können, wenn Namensidentität zwischen der juristischen und der dahinstehenden natürlichen Person besteht.[44] Bei kleineren landwirtschaftlichen Betrieben, die als juristische Person organisiert sind, kann sich über die Bezeichnung oder Anschrift des landwirtschaftlichen Betriebs ein Personenbezug ergeben, wenn hinter der juristischen Person eine Einzelperson steht.[45]

2. Bestimmung des Verantwortlichen

Art. 4 Nr. 7 DSGVO bestimmt als Verantwortlichen "die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Nach Art. 4 Nr. 8 DSGVO ist "eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet" nur Auftragsverarbeiter. Bei der Beteiligung mehrerer Personen kann auch eine gemeinsame Verantwortlichkeit bestehen (Art. 26 I 1 DSGVO).[46] Bei der Beurteilung der Verantwortlichkeit wird in der Literatur zumeist zwischen der öffentlichen und privaten Blockchain unterschieden.

a) Öffentliche Blockchain

Wegen der dezentralen Struktur der Blockchain kann „nicht auf eine konkrete Person oder Einrichtung abgestellt werden, die die alleinige Entscheidungsmacht über die Verarbeitung der Daten innehat."[47] Daher wird es für möglich gehalten, dass bei einer öffentlichen Blockchain entweder alle oder keiner der Netzwerkteilnehmer als Verantwortliche nach Art. 4 Nr. 7 DSGVO anzusehen sind.[48] Beide Ergebnisse werden als nicht zielführend angesehen.[49] Ob eine Verantwortlichkeit vorliegt wird zum Teil danach beurteilt, welche Rolle die Netzwerkteilnehmer innehaben. So sollen bei der öffentlichen Blockchain die Absender einer Transaktion Verantwortliche sein, weil diese über die Aufnahme von neuen Daten in die Blockchain entscheiden.[50] Alle Teile der Wertschöpfungskette würden bei dem Einsatz der Blockchain jeweils Absender von Transaktionen sein. Damit bedürfte es für alle Teile der Wertschöpfungskette des Vorliegens eines Erlaubnistatbestandes zur Datenverarbeitung.

b) Private Blockchain

Nach einer Auffassung sollen bei der privaten (zulassungsbegrenzten) Blockchain derjenige, der über die Zuteilung der Zugangsrechte bestimmt, alleiniger Verantwortlicher und die restlichen Netzwerkteilnehmer Auftragsverarbeiter (Art. 4 Nr. 8, Art. 28 DSGVO) sein.[51] Daher sei bei der privaten Blockchain die handelnde Behörde allein verantwortlich, wenn der Staat eine Blockchain einsetzt.[52] Eine andere Ansicht sieht die Absender von Transaktionen dann als Verantwortliche an, wenn diese autonom darüber entscheiden, ob personenbezogene Daten verarbeitet werden.[53] Wenn die vorgenommene Transaktion aufgrund des durch eine zentrale Instanz vorgegebenen Zwecks personenbezogene Daten beinhaltet und als Aufgabe der zentralen Instanz erfolgen, dann soll hingegen nur eine Auftragsverarbeitung vorliegen.[54] Im Falle der Kontrolle von Wertschöpfungsketten durch die Verwaltung würde der Zweck der Datenverarbeitung (Transparenz der einzelnen Produktionsschritte) durch die Behörde bestimmt werden. Nach § 39 I 1 LFGB ist die Einhaltung der Vorschriften des LFGB Aufgabe der zuständigen Behörde. Die Lebensmittelunternehmer sind zwar auch zur Selbstkontrolle verpflichtet,[55] aber der Zweck der Blockchain wäre eben die transparente Sichtbarmachung der gesamten Wertschöpfungskette. Dieser Zweck wäre durch die zuständige Behörde festgelegt worden. Daher wäre nach beiden Ansichten die Behörde alleinige Verantwortliche.

In einer privaten Blockchain, an der nur die Akteure der Wertschöpfungskette beteiligt sind, würde hingegen eine Verantwortlichkeit von allen Nutzern in Betracht kommen, denn in diesem Szenario würde der Zweck der Datenverarbeitung (Selbstkontrolle der Lebensmittelunternehmer) regelmäßig durch alle Teilnehmer gemeinsam festgelegt werden.

3. Rechtmäßigkeit der Datenverarbeitung innerhalb der Blockchain

Die Datenverarbeitung ist gemäß Art. 6 I DSGVO dann rechtmäßig, wenn einer der dort aufgezählten Erlaubnistatbestände erfüllt ist. Bei mehreren Verantwortlichen muss für jeden Einzelnen eine Rechtsgrundlage nach Art. 6 I DSGVO vorliegen, welche unterschiedlich oder identisch sein können.[56] Als Rechtsgrundlage für die Datenverarbeitung kommen die Einwilligung (Art. 6 I a DSGVO), Erforderlichkeit für die Erfüllung von Vertragszwecken (Art. 6 I 1 b DSGVO) und überwiegende berechtigte Interessen (Art. 6 I 1 f DSGVO) in Betracht. Ein Verstoß gegen die Grundsätze der Verarbeitung kann nach Art. 84 V a DSGVO ein Bußgeld von 20.000.000 € oder im Fall eines Unternehmens ein Bußgeld

42 Deutscher Bauernverband, Situationsbericht 2018/19 – Betriebs- und Rechtsformen, abrufbar unter: https://www.bauernverband.de/situationsbericht-19/3-agrarstruktur/34-betriebs-und-rechtsformen.
43 Vgl. *Kipker/Bruns*, CR 2020, 210 (211).
44 *EuGH*, Urt. v. 9. 10. 2010, verb. Rs. Volker und Markus Schecke GbR (C-92/0) und Hartmut Eifert (C-93/09)/Land Hessen, ECLI:EU:C:2010:662, Rn. 52.
45 *Kipker/Bruns*, CR 2020, 210 (211).
46 Vgl. *Kipker/Bruns*, CR 2020, 210 (214).
47 *Bechtolf/Vogt*, ZD 2018, 66 (69).
48 Vgl. *Quiel,* DuD 2018, 566 (569 f.); für eine Verantwortlichkeit aller Teilnehmer unabhängig von der konkreten Ausgestaltung der Blockchain: *Schrey/Thalhofer*, NJW 2017, 1431 (1431).
49 Vgl. *Bechtolf/Vogt,* ZD 2018, 66 (69); *Quiel,* DuD 2018, 566 (570).
50 *Janicki/Saive*, ZD 2019, 251 (254); *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).
51 *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).
52 *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).
53 *Janicki/Saive*, ZD 2019, 251 (255).
54 *Janicki/Saive*, ZD 2019, 251 (255).
55 Vgl. *Rathke,* in: *Zipfel/Rathke,* Lebensmittelrecht, 176. EL (2020), Art. 17 BasisVO, Rn. 1.
56 *Petri*, in:*Simitis/Hornung/Spiecker gen. Döhmann,* Datenschutzrecht, 2019, Art. 26 DSGVO, Rn. 1.

von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist, verhängt werden.

a) Einwilligung in die Verarbeitung nach Art. 6 I a DSGVO

Die Einwilligung in die Datenverarbeitung muss gegenüber allen am Blockchain-Netzwerk Beteiligten erfolgen, weshalb die Einwilligung bei der öffentlichen Blockchain ausscheidet.[57] Eine Einwilligung (gegenüber allen Teilnehmern der Blockchain) kommt deswegen nur dann in Betracht, wenn der Kreis der Teilnehmer von vornherein klar ist und auch keine weiteren Teilnehmer nach der Einwilligung hinzutreten. Diese Anforderung kann nur eine private Blockchain erfüllen, deren Teilnehmerzahl sich nicht erhöht. Zudem muss die Einwilligung für einen oder mehrere bestimmte Zwecke abgegeben werden.[58] Zudem wird eingewandt, dass beim Einwilligenden eine hinreichende Kenntnis über die Tragweite der Datenverarbeitung bestehen müsse und dass eine solche hinreichende Kenntnis dem durchschnittlichen Verbraucher fehlen würde.[59] Beim Einsatz der Blockchain in der Überwachung der Wertschöpfungskette setzen alle Netzwerkteilnehmer die Blockchain-Technologie ein. Deswegen kann in diesem Fall davon ausgegangen werden, dass alle Teilnehmer über ein hinreichendes Wissen über die Datenverarbeitung verfügen.

An der für die Wirksamkeit einer Einwilligung erforderliche Freiwilligkeit (Art. 4 Nr. 11 DSGVO) kann es dann fehlen, wenn zwischen dem Verantwortlichen und der betroffenen Person ein klares Ungleichgewicht besteht.[60] Da die Behörde als Hoheitsträger gegenüber Privaten auftrete, befänden diese sich in einem Über- / Unterordnungsverhältnis. [61] Dies werde durch den Erwägungsgrund 43 der DSGVO gestützt, der es als Fall des klaren Ungleichgewichts bezeichnet, wenn die Verantwortliche eine Behörde ist.[62] Der Erwägungsgrund setzt aber weiter voraus, dass "es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde". Die zuständigen Behörden haben sich gemäß § 39 I 1 LFGB „durch regelmäßige Überprüfungen und Probennahmen davon zu überzeugen, dass die Vorschriften" (gemeint sind solche der Lebensmittelsicherheit) "eingehalten werden." Durch den Einsatz der Blockchain geben die Lebensmittelunternehmer den Behörden gegenüber mehr Informationen preis, als diese sonst durch regelmäßige Kontrollen erhalten würden. Die Unternehmen könnten also ein Interesse daran haben, weniger Informationen an die Behörden zu übermitteln, als sie dies beim Einsatz der Blockchain tun. Aus Sicht der Unternehmen liegt es nahe, dass eine verweigerte Einwilligung zu verstärkten Kontrollen ihres Betriebes führen kann, weil der Anschein der Nichteinhaltung von Lebensmittelrechtlichen Vorschriften erweckt werden könne. Deshalb kann ein genereller Zweifel an der Freiwilligkeit der Einwilligung im Verhältnis Lebensmittelunternehmer und Behörde bestehen. Ob dies im Einzelnen der Fall ist, ist für die Behörde wahrscheinlich typischerweise nicht zu erkennen. Daher geht mit der Einwilligung immer ein Grad an Unsicherheit einher.

Nach Art. 7 III 1 DSGVO kann die Einwilligung jederzeit widerrufen werden. Der Widerruf wirkt *ex nunc* (Art. 7 III 2 DSGVO). Bei erfolgtem Widerruf könnte die Blockchain nicht fortgesetzt werden, weil die Daten bei jeder neuen Transaktion in der Blockchain wieder verarbeitet werden würden.[63] Deswegen muss ein weiteren Erlaubnistatbestand nach Art. 6 I DSGVO erfüllt sein, um eine ununterbrochene Transparenz der Wertschöpfungskette sicherzustellen. Die Verarbeitung sollte deshalb niemals nur auf die Einwilligung gestützt werden.

b) Verarbeitung zur Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen nach Art. 6 b DSGVO

Die Verarbeitung ist nach Art. 6 b DSGVO dann rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. In diesem Fall muss die betroffene Person auch Partei des Rechtsverhältnisses sein.[64] Deswegen können sich nur die Netzwerkteilnehmer auf den Erlaubnistatbestand berufen, die mit der betroffenen Person in (vor-)vertraglicher Verbindung stehen. In der Wertschöpfungskette werden regelmäßig immer nur die Teile in einer vertraglichen Rechtsbeziehung stehen, deren Arbeitsprozesse aneinander anknüpfen. Daher können sich die übrigen Teilnehmer wohl regelmäßig nicht auf Art. 6 b DSGVO berufen.

c) Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 c DSGVO

Die rechtliche Verpflichtung kann aus dem Unions- oder dem nationalen Recht stammen und muss kein Parlamentsgesetz sein.[65] Die Rechtsgrundlage, die die Verpflichtung festlegt, muss nach Erwägungsgrund 41 der DSGVO aber hinreichend klar, präzise und vorhersehbar sein und insbesondere den Zweck der Verarbeitung festlegen.[66] Auch Behörden können sich auf Art. 6 c DSGVO berufen, wenn es sich nicht um die Verarbeitung für eine öffentliche Aufgabe handelt.[67] Es handelt sich insbesondere dann um eine öffentliche Aufgabe, wenn die Norm Befugnisse mit Ermessens- oder Beurteilungsspielraum einräumt.[68] Als Rechtsgrundlage kommt § 39 I LFGB in Betracht. Nach Satz 1 ist die Überwachung der Einhaltung der Vorschriften des LFGB Aufgabe der zuständigen

57 *Schrey/Thalhofer*, NJW 2017, 1431 (1434).
58 *Schantz*, in: *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht, 2019, Art. 6 DSGVO, Rn. 8.
59 *Quiel*, DuD 2018, 566 (571).
60 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Die DSGVO in der Bundesverwaltung, 2018, 37.
61 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Die DSGVO in der Bundesverwaltung, 2018, 37.
62 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Die DSGVO in der Bundesverwaltung, 2018, 37.
63 Vgl. *Quiel*, DuD 2018, 566 (571).
64 Vgl. *Egberts/Monschke*, JURA 2018, 1100 (1105).
65 *Heberlin in: Ehmann/Selmayr*, DS-GVO, 2. Aufl. (2018), Art. 6, Rn. 15.
66 Vgl. *Heberlin* (o.Fußn. 65), Art. 6, Rn. 15.
67 *Heberlin* (o.Fußn. 65), Art. 6, Rn. 15.
68 *Heberlin* (o.Fußn. 65), Art. 6, Rn. 15.

Behörden. Satz 2 bestimmt, dass die Behörden "sich durch regelmäßige Überprüfungen und Probennahmen davon zu überzeugen, dass die Vorschriften eingehalten werden." Wobei das Wort regelmäßig einen behördlichen Beurteilungsspielraum impliziert. Damit scheidet § 39 I LFGB als Rechtsgrundlage nach Art. 6 c DSGVO aus.

Die Lebensmittelunternehmer müssen Daten, von dem in der Versorgungskette jeweils vor- oder nachgelagerten Unternehmen speichern, um den Aufzeichnungspflichten für eine Rückverfolgbarkeit nachzukommen.[69] Art. 17 Lebensmittel-Basisverordnung verpflichtet die Lebensmittelunternehmer, die Einhaltung der Lebensmittelrechtlichen Vorgaben durch regelmäßige und umfangreiche Prüfungen, sicherzustellen.[70] Aus Art. 18 Lebensmittel-Basisverordnung ergibt sich, dass die Lebensmittelunternehmer verpflichtet sind zu dokumentieren, wohin welche Lebensmittel geliefert werden[71] und woher ihre Lebensmittel und Rohstoffe stammen.[72] Auf die Erfüllung dieser rechtlichen Verpflichtungen können sich daher nur diejenigen Teilnehmer berufen, die in einem Vertragsverhältnis stehen.[73]

d) Erforderlichkeit der Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 e DSGVO)

Ob eine Aufgabe im öffentlichen Interesse besteht, die eine Verarbeitung erfordert, ergibt sich aus einer unionalen oder nationalen Rechtsgrundlage.[74] Als Rechtsgrundlage der Datenverarbeitung kommt § 39 I 2 LFGB in Betracht, welche die Behörden zu regelmäßigen Kontrollen der Lebensmittelunternehmer verpflichtet. Der Einsatz der Blockchain zur Sichtbarmachung der Wertschöpfungskette führt dazu, dass eine dauerhafte Überwachung durch die Behörden ermöglicht wird, wenn diese an der Blockchain beteiligt sind. § 39 I 2 LFGB spricht aber von regelmäßigen Überprüfungen. Eine dauerhafte Überprüfung der Vorschriften kennt das Gesetz gerade nicht. Wenn die dauerhafte Überprüfung nicht zulässig ist, dann kann die Verarbeitung der Daten, einer dauerhaften Überprüfung ebenfalls nicht zulässig sein. Deshalb kann die Norm nicht als Grundlage für Datenverarbeitung herangezogen werden. Eine andere Norm kommt nicht in Betracht.

e) Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten nach Art. 6 I f DSGVO

Nur Private können sich auf den Erlaubnistatbestand aus Art. 6 f DSGVO berufen, weil Art. 6 I UAbs. 2 DSGVO die Anwendbarkeit für Behörden ausschließt, wenn sie in Erfüllung ihrer Aufgaben handeln.[75] Die Norm besteht aus den drei Tatbestandmerkmalen: Interesse des Verantwortlichen oder eines Dritten, Erforderlichkeit der Verarbeitung zur Interessenerreichung und kein Überwiegen der berechtigten Interessen des Betroffenen.[76]

aa.) Interesse des Verantwortlichen oder eines Dritten. Das Vorliegen eines berechtigten Interesses, ist „rein normativ zu entscheiden und zunächst unter Berücksichtigung des Zwecks der Verarbeitung zu beurteilen.“[77] Das Interesse des Verantwortlichen kann rechtlicher, wirtschaftlicher oder ideeller Natur sein.[78] Die Lebensmittelunternehmer haben alle ein Interesse an der Sicherheit ihrer Produkte. Dieses Interesse ist rechtlicher Natur, weil sie nach Art. 17 Lebensmittel-Basisverordnung zur Einhaltung der Lebensmittelrechtlichen Vorgaben verpflichtet sind. Dieses Interesse hat auch eine wirtschaftliche Komponente, weil eine transparente Lieferkette dazu führt, dass die Quelle von Verunreinigungen schneller gefunden werden können. Deshalb ist es durch den Einsatz der Technologie eher möglich, ein schädliches Produkt zu identifizieren und eine Produkthaftung zu vermeiden.

bb.) Erforderlichkeit. Die Datenverarbeitung ist dann nicht erforderlich, wenn die Interessen auf eine andere gleich wirksame Weise verwirklicht werden können, die die Interessen des Betroffenen weniger beeinträchtigt.[79] Der Einsatz einer Blockchain ermöglicht eine effektivere Transparenz und Rückverfolgbarkeit, die andere Technologien nicht in dem selben Maß bereitstellen können. Der Einsatz der Technologie wäre damit erforderlich.

cc) kein Überwiegen der Interessen des Betroffenen. Die Interessen des Betroffenen dürfen nicht überwiegen. Sind die Interessen des Betroffenen und Verarbeitenden allerdings gleichwertig, fehlt es an einem Überwiegen und die Verarbeitung ist rechtmäßig.[80] Den europäischen Grundrechten und Grundfreiheiten kommt bei der Gewichtung der Interessen eine besondere Bedeutung zu.[81] Die betroffene Person ist durch die Datenverarbeitung in ihren Grundrechten auf Achtung des Privat- und Familienlebens (Art. 7 GRCh) und Schutz personenbezogener Daten (Art 8 GRCh) betroffen.[82] Dem gegenüber stehen die Berufsfreiheit (Art. 15 I GRCh) und die Unternehmerische Freiheit (Art. 16 GRCh) der Verarbeitenden. Die Grundrechte der betroffenen Person sind hier deswegen geringer zu gewichten, weil ihre Vertragspartner schon zur Verarbeitung ihrer Daten gesetzlich verpflichtet sind. Die Verarbeitung durch weitere Teile der Lieferkette stellt deswegen einen eher geringen Eingriff dar. Die Interessen der Betroffenen überwiegen deshalb nicht.

69 *Kipker/Bruns*, CR 2020, 210 (214).
70 Vgl. *Scherzberg/Garbe*, ZLR 2018, 198 (212).
71 *Scherzberg/Garbe*, ZLR 2018, 198 (214).
72 *Meyer in: Meyer/Streinz*, LFGB – BasisVO, 2. Aufl. (2012), Art. 18 BasisVO, Rn. 15.
73 Vgl. *Kipker/Bruns*, CR 2020, 210 (214).
74 *Roßnagel,* in: *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht, 2019, Art. 6 DSGVO, Rn. 71.
75 Vgl. *Albers/Veit,* in: *Wolff/Brink,* BeckOK Datenschutzrecht, 33. Aufl. (2020), Art. 6 DSGVO, Rn. 46.
76 Vgl. *Egberts/Monschke,* JURA 2018, 1100 (1105).
77 *Albers/Veit,* in: *Wolff/Brink,* BeckOK Datenschutzrecht, 33. Aufl. (2020), Art. 6 DSGVO, Rn. 49.
78 *Schulz,* in: *Gola,* DSG-VO, 2. Aufl. (2018), Art. 6, Rn. 57.
79 *Schantz,* in: *Simitis/Hornung/Spiecker gen. Döhmann,* Datenschutzrecht, 2019, Art. 6 Rn. 100.
80 *Schulz* (o.Fußn. 78), Art. 6, Rn. 58.
81 *Schulz* (o.Fußn. 78), Art. 6, Rn. 59.
82 Vgl. *Schantz,* in: *Simitis/Hornung/Spiecker gen. Döhmann,* Datenschutzrecht, 2019, Art. 6 Rn. 101.

4. Recht auf Vergessenwerden (Art. 17 DSGVO)

Das Recht auf Vergessenwerden führt nach Art. 17 I DSGVO dazu, dass der Verantwortliche die personenbezogenen Daten unverzüglich löschen muss. Nach Art. 17 I b DSGVO entsteht eine Löschungspflicht, wenn die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 I a DSGVO stützte, widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt. Ein Verstoß gegen die Löschungspflicht kann nach Art. 83 V b DSGVO zur Verhängung einer Geldbuße führen.[83]

Die der Blockchain-Technologie immanente Eigenschaft der Unveränderbarkeit der Daten steht im Konflikt mit dem Recht auf Vergessenwerden (Art. 17 DSGVO),[84] weil bei der klassischen Konzeption der Blockchain eine nachträgliche Löschung technisch nicht möglich ist.[85] Zur Lösung des Problems werden einige technische Modifikationen der Blockchain vorgeschlagen, die aber zu Folgeproblemen führen. Durch „Pruning" können alte Blöcke aus der Blockchain entfernt werden, wenn das Ergebnis des Blockes zum Ausgangspunkt einer neuen Transaktion innerhalb der Blockchain geworden ist, was aber dazu führt, dass Nachvollziehbarkeit und Fälschungssicherheit der Blockchain eingeschränkt werden und dadurch die Vertrauenswürdigkeit der Technologie gemindert wird.[86] Eine nachträgliche Anonymisierung von personenbezogenen Daten kann nicht gewährleisten, dass alle denkbaren Identifizierungswege aufgehoben werden.[87] Eine weitere Möglichkeit ist die Verschlüsselung von personenbezogenen Daten innerhalb der Blockchain, wobei der „Entschlüsselungskey" außerhalb der Blockchain gespeichert wird, denn dann können durch die Löschung eben dieses „Entschlüsselungskeys" die personenbezogene Daten faktisch unzugänglich gemacht werden – was zur Unlesbarkeit führt.[88] Aber um das datenschutzrechtliche Erfordernis der Löschung zu erfüllen muss auch beachtet werden, ob die Information (ggf. unter Zuhilfenahme von Spezialtechnologie) wiederhergestellt werden kann.[89] Schon nach dem jetzigen Stand der Technik ist eine Entschlüsselung nach dem Löschen des „Entschlüsselungskeys" zwar zeitaufwendig, aber technisch möglich.[90] Schließlich wird noch die Pseudonymisierung als Ansatz vorgeschlagen, bei dem die Namen auch lediglich außerhalb der Blockchain gespeichert werden.[91] Bei diesem Verfahren soll aber die Identifizierung mittels Big-Data-Verfahren möglich sein.[92]

Ein rechtlicher Lösungsvorschlag ist, dass der nationale Gesetzgeber das Löschungsrecht nach § 23 I e DSGVO zurückstuft.[93] Die Vorschrift erlaubt durch Gesetzgebungsakt von den Rechten nach Art. 12 – 22 DSGVO abzuweichen, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt: e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit". In Verbindung mit Erwägungsgrund 73 DSGVO werde den nationalen Gesetzgebern insbesondere das Recht zugestanden, für „das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses" Abweichungen von Art. 17 I DSGVO zuzulassen.[94] Im Vergleich zu klassischen Serverlösungen eröffne eine Blockchain ein höheres Potenzial, manipulative Eingriffe in die Datenstruktur zu verhindern, zudem könne sie Verwaltungsprozesse beschleunigen und durch den Wegfall von Schnittstellen Kosten einsparen.[95] Wenn der erzielte Nutzen die Persönlichkeitsrechte der Betroffenen überwiege, dann sei eine mitgliedstaatliche Einschränkung des Rechts auf Vergessenwerden gerechtfertigt.[96] Die bessere Überwachung der Wertschöpfungsketten im Lebensmittelsektor dient vor allem dem Gesundheitsschutz der Verbraucher. Eine Steigerung des Gesundheitsschutzes dürfte den Persönlichkeitsrechtsschutz überwiegen, weil es sich meist um Daten handelt, die die Betroffenen im Rahmen der betrieblichen Kontrolle an die Behörden übermitteln müssen.

IV. Fazit

Die zuständigen Behörden können zur Überwachung von Wertschöpfungsketten nicht an einer Blockchain beteiligt sein, wenn in dieser Blockchain personenbezogene Daten verarbeitet werden, weil sich die Behörden nicht auf einen Erlaubnistatbestand nach Art. 6 I DSGVO berufen können. Damit sich die Behörden auf das rechtliche Interesse des Gesundheitsschutzes nach Art. 6 e DSGVO berufen können, bedürfte es einer gesetzlichen Änderung der Überprüfungspflichten nach § 39 I 2 LFGB.

Der Einsatz der Blockchain durch Private ist hingegen datenschutzrechtlich zulässig. Daher wäre es denkbar, dass die Teilnehmer der Wertschöpfungskette die Daten in einer Blockchain speichern und die Behörde gezielt auf diese zugreift. Dies könnte etwa zur regelmäßigen Überprüfung nach § 39 I 2 LFGB oder zur Feststellung eines Verstoßes gegen die Lebensmittelrechtlichen Vorgaben erfolgen. Eine gesetzliche Verpflichtung zur Einrichtung solcher privaten Blockchains besteht derzeit aber nicht. Denkbar wäre es, dass der Gesetzgeber hier tätig wird und die bestehenden Aufzeichnungspflichten an den Einsatz der Technologie knüpft oder dass gezielt Anreize zum Einsatz der Technologie geschaffen werden.

83 *Paal,* in: *Paal/Pauly*, DS-GVO BDSG, 2. Aufl. (2018), Art. 17 DSGVO, Rn. 19.
84 *Martini/Weinzierl*, NVwZ 2017, 1251 (1252); *Kipker/Bruns*, CR 2020, 210 (215).
85 *Schrey/Thalhofer*, NJW 2017, 1431 (1435).
86 *Martini/Weinzierl*, NVwZ 2017, 1251 (1255).
87 *Martini/Weinzierl*, NVwZ 2017, 1251 (1256).
88 *Kipker/Bruns*, CR 2020, 210 (216).
89 *Dix,* in: *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht, DSGVO Art. 17 Recht auf Löschung („Recht auf Vergessenwerden"), 2019, Rn. 5.
90 *Kipker/Bruns*, CR 2020, 210 (216).
91 *Kipker/Bruns*, CR 2020, 210 (216).
92 *Martini/Weinzierl*, NVwZ 2017, 1251 (1256).
93 *Martini/Weinzierl*, NVwZ 2017, 1251 (1258).
94 *Martini/Weinzierl*, NVwZ 2017, 1251 (1258).
95 *Martini/Weinzierl*, NVwZ 2017, 1251 (1258).
96 *Martini/Weinzierl*, NVwZ 2017, 1251 (1258).