NutriSafe

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

IGMR

der Bundeswehr Universität München

NutriSafe Toolkit

– Rechtlicher Rahmen –

Data Governance im Rahmen von NutriSafe: Rechtliche und organisatorische Anforderungen

Dr. Dennis-Kenji Kipker

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Bundesministerium Landwirtschaft, Regionen und Tourismus

SIFO.de

KIRAS Sicherheitsforschung

FFG Forschung wirkt.

Dieses Dokument ist Bestandteil im **NutriSafe Toolkit**:

nutrisafe.de/toolkit

In einer Kooperation zwischen Deutschland und Österreich forschen Universitäten, Unternehmen und Behörden daran, die Lebensmittelproduktion sowie deren Logistik unter Nutzung von Distributed-Ledger-Technologie sicherer zu machen.

Das Projekt NutriSafe wird auf Österreichischer Seite innerhalb des Sicherheitsforschungs-Förderprogramms KIRAS durch das Bundesministerium für Landwirtschaft, Regionen und Tourismus (BMLRT) gefördert (Projektnummer: 867015). Auf Deutscher Seite wird das Projekt innerhalb des Programms Forschung für die zivile Sicherheit vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (FKZ 13N15070 bis 13N15076).

nutrisafe.de | nutrisafe.at

Data Governance im Rahmen von NutriSafe: Rechtliche und organisatorische Anforderungen

Dr. Dennis-Kenji Kipker[1]

[1]Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

sowie

Institut für Schutz und Zuverlässigkeit, Universität der Bundeswehr München

Bremen und München 2021

1 Allgemeine rechtliche Rahmenbedingungen und deren Bewertung

Im Rahmen der technischen Umsetzung der Blockchain sind verschiedene juristische Anforderungen zu beachten und umzusetzen, so primär datenschutzrechtliche Vorgaben und gesellschaftsrechtliche Rahmenbedingungen zur Implementierung der Blockchain. Mit Blick auf die beteiligten Partner sind somit entsprechende vertragliche Maßnahmen zu realisieren. Ausgegangen wird dabei von der Prämisse, dass für die im Projekt NutriSafe entwickelten Lösungen personenbezogene Daten verarbeitet werden und verschiedene Stellen im Wesentlichen gleichermaßen für die Einhaltung der Rechtmäßigkeit der Datenverarbeitung verantwortlich sind. Damit gelten auch die Anforderungen, die die DS-GVO im Umgang mit den datenschutzrechtlichen Betroffenenrechten festschreibt, denn die in der entwickelten Lösung generierten Blockchain-Daten werden in einer sog. „Permitted Community“ verarbeitet, sodass im Regelfall due Zuordenbarkeit zu natürlichen Personen gegeben sein wird.

Für die Blockchain gilt, dass in technischer Hinsicht ein dezentrales System eingerichtet wird. Im datenschutzrechtlichen Sinne wird man für diese Fälle regelmäßig eine „joint controllership“ annehmen können, die sich nach Art. 26 DS-GVO richtet. Dies setzt den Abschluss eines Vertrags voraus, in dem die Parteien in transparenter Form festlegen, wer von ihnen welche Verpflichtung gem. der DS-GVO erfüllt – uns insbesondere auch, wer Anlaufstelle für die betroffene Person ist, deren Daten verarbeitet werden. Die zu treffende Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsamen Verantwortlichen gegenüber den betroffenen Personen gebührend widerspiegeln. Für NutriSafe wird entsprechenderweise empfohlen, eine gemeinsame Vereinbarung in der Form von Allgemeinen Geschäftsbedingungen (AGB) zu treffen, wobei die Erfüllung der datenschutzrechtlichen Betroffenenrechte für die einzelnen Partner intern durch diese festgeschrieben wird. Bei der Zulassung zum Blockchain-System tritt jeder neue Teilnehmer der AGB-Vereinbarung durch entsprechende Zustimmung bei.

Soweit es die datenschutzrechtlichen Fragestellungen für den Betrieb der Blockchain anbelangt, bedarf es einer Rechtsgrundlage zur Datenverarbeitung, da für den Fall von NutriSafe wie zuvor bereits festgestellt personenbezogene Daten verarbeitet werden. Art. 6 DS-GVO sieht in diesem Zusammenhang eine Reihe von Legitimationstatbeständen vor, so

unter anderem die datenschutzrechtliche Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DS-GVO) und die Datenverarbeitung zur Erfüllung von Vertragszwecken (Art. 6 Abs. 1 S. 1 lit. b DS-GVO). Die Einholung der Einwilligung dürfte auf den konkret zu beurteilenden Fall zugeschnitten ein unpraktikables Instrument für eine Legitimierung der Datenverarbeitung sein, da nicht nur eine Vielzahl noch unbestimmter Akteure an der Blockchain beteiligt ist, sondern die Einwilligung auch jederzeit widerrufen werden kann. Für die Anwendungsszenarien von NutriSafe dürfte demgegenüber vor allem ein Interesse an der Vertragserfüllung bestehen, so beispielsweise mit Blick auf Serviceverträge. Vorrangig ist für die rechtliche Legitimation zur Verarbeitung personenbezogener Daten in der Blockchain deshalb der Erlaubnistatbestand aus Art. 6 Abs. 1 S. 1 lit. b DS-GVO heranzuziehen.

Eine weitere, für die Implementierung der Blockchain relevante Fragestellung betrifft das Urheberrecht. Hier gilt im Grundsatz, dass die Blockchain rechtlich als ein privates Register ohne besondere eigenständige gesetzliche Vorgaben zu qualifizieren ist. Ziel der Blockchain ist, Informationen fälschungssicher aufzulisten und den verschiedenen, daran beteiligten Parteien zur Nachvollziehbarkeit von Logistikketten im Lebensmittelsektor zugänglich zu machen. Fraglich ist somit, ob an diesen Informationen ein geistiges Eigentumsrecht besteht. Grundsätzlich gilt in dem Zusammenhang, dass eine bloße Auflistung von Informationen nicht als urheberrechtliches Werk zu qualifizieren ist, da es an der von § 2 UrhG vorausgesetzten Schöpfungshöhe fehlt. Dem Urheberrechtsschutz unterfallen aber auch Datenbanken. Eine Datenbank ist gem. § 87a UrhG eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Dabei gilt gem. § 87a Abs. 2 UrhG derjenige als Datenbankhersteller im Sinne des Gesetzes, der die Investition in die Datenbank vorgenommen hat. Bei der Beurteilung, ob die NutriSafe-Blockchain eine Datenbank ist, kommt es somit auf eine Einzelfallbetrachtung der konkreten Implementierung an. Jedenfalls dürfte dann keine urheberrechtlich geschützte Datenbank vorliegen, wenn die Blockchain ein bloßes elektronisches Mittel für eine Datensammlung darstellt.

Eine abschließende zentrale rechtliche Fragestellung für die Data Governance von NutriSafe betrifft die Einordnung der Blockchain als Rechtssubjekt. Allein durch separates Einpflegen von Daten in die Blockchain wird per se zunächst keine Gesellschaft begründet. Anzudenken wäre hier jedoch, dass es sich bei dem Zusammenschluss der beteiligten Parteien zu einem Peer-to-Peer-Netzwerk um eine Innengesellschaft nach § 705 BGB handelt. Im Rahmen einer solchen Gesellschaft verpflichten sich die Gesellschafter durch den Gesellschaftsvertrag gegenseitig, die Erreichung eines gemeinsamen Zweckes in der durch den Vertrag bestimmten Weise zu fördern, insbesondere die vereinbarten Beiträge zu leisten. Für den vorliegenden Fall könnte der für eine Innengesellschaft benötigte gemeinsame Zweck in der gemeinsamen Blockchain-Verwaltung bestehen. Dies ist rechtlich aber nicht unstreitig und von der Höhe der vereinbarten Zweckförderung abhängig: Für den praktizierten Regelfall nehmen die Nutzer an einem Blockchain-Netzwerk nicht unbedingt am Netzwerk teil, um sich gegenüber anderen zu dessen Verwaltung zu verpflichten, sondern in erster Linie nur, um dieses für sich zu nutzen. Bei einer solchen praxisorientierten Betrachtung fehlt folglich grds. der Rechtsbindungswille bei den Teilnehmern an der Blockchain. Außerdem dehnt die pauschale Annahme einer Innengesellschaft den Anwendungsbereich der BGB-Gesellschaft über Gebühr aus. Als gesellschaftsrechtliche Alternative in Betracht zu ziehen wäre noch die Gemeinschaft gem. § 741 BGB, deren Regelungen Anwendung finden, soweit mehreren ein Recht gemeinschaftlich zusteht. Für diesen Fall finden die Vorschriften der §§ 742-758 BGB Anwendung. Unter anderem wird für diesen Fall bestimmt, dass im Zweifel den Teilnehmern gleiche Anteile zustehen, und jedem Teilhaber ein seinem Anteil entsprechender Bruchteil der Früchte gebührt. Auch diese Rechtsform muss aber letztlich ausscheiden, da eine Blockchain in ihrer Gesamtheit regelmäßig kein Recht darstellen dürfte und folglich auch keine Gemeinschaft an ihr begründet werden kann.

Im Ergebnis ist die Blockchain somit als privates Register ohne Rechtseigenschaft zu definieren. Dennoch kann ein schuldrechtliches Recht bzw. ein Anspruch auf Eintragung in der Blockchain vereinbart werden, dies wie oben dargelegt vorzugsweise mittels Servicevertrag/AGB.

2 Relevante rechtliche Einzelfragen im chronologischen Nutzungsverlauf der Blockchain

1. Was ist bei der Begründung eines Blockchain-Konsortiums mit Blick auf die Auswahl des Betreibermodells zu beachten?

Für den Betrieb der Blockchain ist keine Gründung eines Konsortiums mit allen Teilnehmern erforderlich.

Aufgrund von Haftungsfragen könnte es aber sinnvoll sein, für den technischen Betrieb der Blockchain eine Gesellschaft mit beschränkter Haftung (GmbH) zu begründen. Diese Wahl einer Rechtspersönlichkeit ist aber nicht zwingend.

2. Wie gestaltet sich rechtlich das sog. „On-Boarding", also die Aufnahme von neuen Mitgliedern, Akteuren etc.?

Eintragungen in die Blockchain sind als technische Handlung rechtlich gesehen zunächst ein sog. „Realakt" ohne grundsätzliche juristische Relevanz.

Der rechtliche „Beitritt" zur Blockchain erfolgt durch individuelle Verträge mit den jeweiligen Mitgliedern, diese können der Prozessvereinfachung halber in der Form von Allgemeinen Geschäftsbedingungen (AGB) ausgestaltet sein.

Die AGB können die relevanten technischen Rechte und Pflichten beinhalten, und außerdem unter Umständen anfallende Nutzungsgebühren, die als Dauerschuldverhältnis abgewickelt werden.

Bei der Aufnahme neuer Mitglieder in die Blockchain darf insbesondere für das Szenario von NutriSafe die datenschutzrechtliche Komponente nicht außer Acht gelassen werden: Soweit personenbezogene Daten verarbeitet werden, muss eine gemeinsame datenschutzrechtliche Verantwortlichkeit zwischen dem technischen Betreiber und den einzelnen Parteien begründet werden. Diese sog. „joint controllership" gem. Art. 26 DS-GVO setzt voraus, dass in einer (vertraglichen) Vereinbarung in transparenter Form festgelegt wird, welcher Verantwortliche welche Verpflichtung gemäß der DS-GVO erfüllt. Dabei sind insbesondere rechtliche und technisch-organisatorische Umsetzungsanforderungen zur Erfüllung der

datenschutzrechtlichen Betroffenenrechte zu beachten, da im NutriSafe-Szenario regelmäßig auch personenbezogene Daten in der Blockchain verarbeitet werden dürften.

3. Wer trifft im operativen Betrieb der Blockchain die relevanten Entscheidungen?

Bei der rechtlichen Würdigung zunächst nicht von Relevanz ist die Zuordnung bloßer gesellschaftsrechtlicher Organfunktionen wie Vorstand, Geschäftsführer etc.

Vielmehr ergeben sich die Rechtspflichten im Einzelnen aus den Vertragsbeziehungen der einzelnen Parteien zueinander. Aufgrund der dezentralen technischen Ausrichtung der Blockchain hat dabei im operativen Betrieb zunächst keine Partei „das letzte Wort".

Gleichwohl kann im Servicevertrag/in den AGB zum Blockchain-Betrieb ein Rechte- und Pflichtenkatalog inkl. Sanktionen festgeschrieben werden, und den Parteien in der Blockchain kann auf diese Weise beispielsweise bei wiederholten Zuwiderhandlungen gegen die Teilnahmebestimmungen ihre Mitgliedschaft gekündigt werden.

4. Wer hat das „Eigentum" an den Daten in der Blockchain und was passiert mit den Daten, die in die Blockchain eingepflegt wurden?

Zur Beantwortung dieser Frage ist zwischen dem Datenschutz- sowie dem Urheberrecht zu unterscheiden.

Grds. besteht kein Urheberrecht an den Daten in der Blockchain, da die gesetzlich geforderte Schöpfungshöhe regelmäßig nicht erreicht werden dürfte.

In die Blockchain eingepflegte Datenbestände begründen auch kein sonstiges Recht, da es regelmäßig außerdem am positiven Zuweisungsgehalt fehlen dürfte. Damit ist gemeint, dass die Daten keiner (juristischen) Person zugewiesen sind, sondern ausschließlich in der Blockchain dokumentiert werden. Damit hat die Eintragung in der Blockchain grds. auch keine rechtliche Stellung, sondern ist vielmehr als Realakt zu qualifizieren. Ein Realakt ist per Definition eine rein tatsächliche, nicht rechtsgeschäftliche Handlung, die lediglich auf einen äußeren Erfolg gerichtet ist (der sich aber auch rechtlich auswirken kann). Die Eintragung in der Blockchain ist damit auch kein „Recht" im juristischen Sinne.

Soweit es jedoch um datenschutzrechtliche Fragen geht, sind für die Eintragung in die Blockchain die Anforderungen zu beachten, die sich aus dem Recht auf informationelle Selbstbestimmung ergeben, beispielsweise mit Blick auf die Geltendmachung von datenschutzrechtlichen Betroffenenrechten. Dies betrifft auch die zuvor bereits geschilderte gemeinsame datenschutzrechtliche Verantwortlichkeit, die hier eine Besonderheit darstellt.

5. Was ist für das „Off-Boarding" zu beachten, also wenn ein Mitglied am Blockchain-Konsortium dieses wieder verlassen will?

Der Servicevertrag, der bereits für das On-Boarding aufgesetzt wurde, enthält auch für den Prozess des Off-Boarding die einschlägigen Rechte und Pflichten der Parteien für die technische Nutzung der Blockchain.

Außerdem sieht der Vertrag Regelungen zur (technischen) Durchführung einer möglichen Kündigung vor.

Von zentraler Bedeutung bei der Kündigung ist die datenschutzrechtliche Behandlung von personenbezogenen Daten, die zuvor in die Blockchain eingepflegt wurden. Da der Blockchain in technischer Hinsicht gerade das Prinzip der Unabänderlichkeit einmal hinzugefügter Datenbestände innewohnt, müssen für die Datensparsamkeit und Datenschutzkonformität technisch-organisatorische Maßnahmen vorgesehen werden, die den verlässlichen Wegfall des Personenbezugs gespeicherter Daten ermöglichen. Dies ist insbesondere dann der Fall, wenn die Rechtsgrundlage zur Datenverarbeitung z.B. mit dem Austritt aus dem Blockchain-Konsortium wegfällt und keine alternativen Erlaubnistatbestände einschlägig sind. In der Rechtswissenschaft diskutiert werden an dieser Stelle unterschiedliche Ansätze, zum Beispiel Pseudonymisierungstechniken und off-chain-Lösungen zur Datenlöschung. In dem Zusammenhang müssen bei einem Off-Boarding auch die weiteren Zugriffsrechte des ursprünglichen Teilnehmers geregelt und ggf. eingeschränkt werden.

6. Wie könnte in der Praxis eine möglichst einfache rechtliche Lösung zur Errichtung eines Blockchain-Konsortiums gestaltet sein?

Die am leichtesten umzusetzende und in der Praxis bislang wohl gängigste Lösung sieht vor, dass nicht mit allen Nutzern und Teilnehmern an der Blockchain umfassende Gesellschaftsverträge geschlossen werden und diese somit auch nicht als direkte Teilhaber anzusehen sind, sondern nur Serviceverträge über die Verwendung von AGB als Dauerschuldverhältnis abgeschlossen werden.

Dabei zu beachten ist, dass ein für eine Gesellschaft regelmäßig gefordertes gemeinsames Interesse aller Teilnehmer an der Blockchain und ihrer Durchführung regelmäßig nicht unterstellt werden kann, sondern gesondert abzuleiten und zu begründen ist. Es gibt somit für den Regelfall auch keinen rechtlichen Automatismus einer Gesellschaftsentstehung allein durch faktisches Handeln.

Regelmäßig dürfte nur für den technischen Betreiber der Gesellschaft, d.h. derjenigen Einrichtung, die die technisch-organisatorischen Ressourcen für das Funktionieren der Blockchain zur Verfügung stellt, eine haftungsbegrenzende Gesellschaftsgründung Sinn machen. Bevorzugte Gesellschaftsform ist hier die Gesellschaft mit beschränkter Haftung (GmbH).

Schon bei Errichtung des Blockchain-Konsortiums sollte der Umgang mit den datenschutzrechtlichen Anforderungen beachtet und klar geregelt werden (vgl. die gemeinsame Verantwortlichkeit gem. Art. 26 DS-GVO). Hier können insbesondere auch Lösungen von Privacy by Design und Privacy by Default (Art. 25 DS-GVO) Berücksichtigung finden.

Danksagung

Besonderer Dank gilt an dieser Stelle Andreas Herrmann von der Universität der Bundeswehr München für seine Unterstützung bei der Vorbereitung der Fallszenarien.