Stand der Bearbeitung: 03.09.2019

Working Paper I:

Der Rechtsrahmen für den praktischen Einsatz der DLT

Dr. Dennis-Kenji Kipker

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)

Universität Bremen

Inhalt:

I. Ziel des Einsatzes der DLT

Gemäß der GVB ist Ziel des Einsatzes der Distributed Ledger Technologie (DLT) die Nachverfolgbarkeit von Güterströmen von der Produktion über die Transport- und Logistikwege bis hin zur Auslieferung an konkrete Endverbraucher. Die Güterströme sollen mithilfe der in der DLT gespeicherten Daten Vertriebsstellen, Logistikrouten, Produktionsstandorten, Produktionszeitpunkten und Maschinen vollumfänglich zuzuordnen sein, wozu es der Speicherung diverser Datenmengen und Datenarten bedarf. Hieraus ergeben sich bereichsübergreifende juristische Anforderungen und Fragestellungen.

II. Funktionsweise der DLT

Bei der DLT werden die Daten – im Unterschied zu einer zentralen Datenbank – dezentral gespeichert.[1] Anders als in klassischen Netzwerken bedeutet Dezentralität hier, dass die Daten nicht von einer Stelle verwaltet werden, sondern jeder Akteur innerhalb eines solchen dezentralen Systems den neuen Datensatz als Kopie in seinem Verzeichnis gespeichert hat. Dabei wird jeder neue Eintrag nach einem bestimmten Verfahren geprüft und in den dezentral bei den Teilnehmern angelegten Datensätzen ergänzt. Eine nachträgliche Änderung oder Löschung soll so im Grundsatz ausgeschlossen und die Integrität der Daten dadurch gewährleistet sein.

III. Grundlegendes zum Rechtsrahmen

Eine Analyse der Vorschriften zeigt, dass im Hinblick auf DLT/Blockchain wenige spezifische Vorschriften existieren. Insoweit ist der Rechtsrahmen, in dem sich diese Technologien bewegen, aus allgemeinen Rechtsvorschriften (sog. Rahmenvorschriften) abzuleiten. Da große Datenmengen – und diese speziell aus dem Bereich der Nahrungsmittelversorgung und Logistik – gespeichert werden, gehören zu diesen allgemeinen Rechtsvorschriften vornehmlich das Datenschutzrecht, teils auch die Regelungen zu Kritischen Infrastrukturen, soweit die durch die BSI-KritisV vorgebenenen zahlenmäßigen Schwellenwerte überschritten werden.

[1] https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444.

Mit Blick auf die gespeicherten Daten ist für das Datenschutzrecht zunächst entscheidend, inwieweit auch *personenbezogene* Daten zur Erfüllung der Zwecke der DLT notwendig wären bzw. inwieweit die gespeicherten Daten die Gefahr bergen, solche Informationen zu umfassen, die Rückschlüsse auf konkrete Personen zulassen und damit u.U. auch personenbezogene Daten darstellen – hier geht es vor allem um die Frage, ob personenbezogenen Daten den Anforderungen genügen, um im Rechtssinne als anonymisiert zu gelten. Soweit es um personenbezogene Daten geht, ist dies sowohl aus datenschutzrechtlicher sowie aus arbeitsrechtlicher Perspektive problematisch und deshalb juristisch näher zu beleuchten. Es sind in diesem Zusammenhang die Voraussetzungen für die Zulässigkeit der Erhebung, Speicherung und Verarbeitung darzustellen und ferner die Anforderungen an die Technologie im Hinblick auf den Umgang mit solchen Daten zu ermitteln.

Durch die Speicherung ergeben sich außerdem Probleme im Hinblick auf die mögliche Angreifbarkeit der Infrastruktur. Aus diesem Grund ist, soweit es sich um eine Kritische Infrastruktur im Sinne des BSIG handelt, ein besonderer Maßstab an den Schutz der Daten vor unbefugtem Zugriff und unberechtigter Datenveränderung anzulegen. Die Anforderung solcher technisch-organisatorischen Schutzvorkehrungen gilt unabhängig von der Frage, ob in einer betroffenen Einrichtung personenbezogene Daten verarbeitet werden.

IV. Datenschutz

Im Hinblick auf das Datenschutzrecht erwachsen insbesondere aus der Dezentralität und der Gestaltung der Zugriffsrechte vielfältige Anforderungen.

a) Begriff des personenbezogenen Datums

Die DS-GVO und das BDSG dienen – neben spezialgesetzlichen Anforderungen und den landesdatenschutzrechtlichen Vorschriften – dem Schutz personenbezogener Daten. Personenbezogene Daten sind ausweislich des Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Demnach sind Daten, die – etwa aufgrund einer Verknüpfung mit dem Klarnamen – unmittelbar einer Person zugeordnet werden können, in jedem Fall personenbezogene Daten. Personenbezogene Daten sind aber auch solche, die etwa nur einem Pseudonym im Zusammenhang mit einer Transaktion im

Block einer blockchain-basierten DLT zugeordnet werden können, sofern es sich eben, im Unterschied zur Anonymisierung, nur um eine Pseudonymisierung handelt, wodurch die Möglichkeit der Zuordnung zu einer realen Person gegeben ist. Bei der Pseudonymisierung werden die tatsächlich identifizierenden Angaben lediglich durch eine allgemeine Kennung ersetzt, die im Zusammenhang mit weiteren Informationen eine zweifelsfreie Zuordnung der betroffenen Personen ermöglicht.

b) Anforderungen an die Erhebung von personenbezogenen Daten

Die DS-GVO macht unterschiedliche Vorgaben zum Erheben, Speichern, Verarbeiten sowie Löschen von Daten. Die Verarbeitung wird dabei gem. der Legaldefinition in Art. 4 Nr. 2 DS-GVO als allgemeiner Oberbegriff aufgefasst, der jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten umfasst. Das Verarbeiten (und damit auch das Erheben) von personenbezogenen Daten bedarf gem. Art. 6 Abs. 1 DS-GVO zur Rechtmäßigkeit einer der dort genannten Voraussetzungen. Dies kann etwa die Einwilligung des Betroffenen (a)), die Notwendigkeit zur Erfüllung einer rechtlichen Verpflichtung (c)), der Schutz lebenswichtiger Interessen (d)) oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse (e)) sein. Hierbei ergeben sich keine besonderen, aus der Eigenart der DLT resultierenden Probleme. Die Daten werden erst nach der Erhebung bzw. in deren Verlauf in die DLT eingeführt. Näher zu untersuchen wäre allenfalls, welche besonderen Rechtmäßigkeitsgründe mit Blick auf das Ziel, den Schutz der (Kritischen) Infrastruktur zu gewährleisten, einschlägig sein könnten.

c) Dezentralität der Datenverarbeitung

Statt einer dezentralen und damit verteilten Verarbeitung von Daten, wie in blockchainbasierten System üblich, hat die DS-GVO eine zentrale Stelle als Verantwortlichen vor Augen. Das führt insoweit zu datenschutzrechtlichen Problemen für den praktischen Einsatz der DLT, als dass nach dem Datenschutzrecht eine primäre Verantwortlichkeit bestimmt werden muss, die aber im Rahmen eines verteilten Systems potenziell gleichrangiger Akteure, welche alle eine Kopie des Datensatzes gespeichert haben, nur schwer bestimmbar ist. Einzig Art. 26 DS-GVO begegnet diesem Umstand, indem er auch im Falle der so genannten „Joint-Control“ eine klare

Verantwortlichkeitsregelung verlangt und Vorgaben zur Zulässigkeit und Ausgestaltung einer solchen Vereinbarung zwischen den einzelnen Akteuren macht.[2] So wird hier bestimmt, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, gemeinsam verantwortlich sind. Dabei haben die Netzwerkbeteiligten eine transparente Vereinbarung zu schließen, die die Verantwortlichkeiten klar regelt.[3] Hierzu bedarf es einer detaillierten Erfassung der Infrastruktur.[4] Auch müssen Regelungen vorgesehen werden, auf welche Weise die datenschutzrechtlichen Betroffenenrechte ausgeübt werden können.

d) Grundsatz der Datenminimierung/Datensparsamkeit

Ein weiterer entscheidender und zu beachtender Grundsatz, der dem Datenschutzrecht zugrunde liegt und in Art. 5 Nr. 1c DS-GVO normiert ist, ist die Datenminimierung, synonym auch als Datensparsamkeit bezeichnet. Nach diesem Grundsatz ist in jedem Stadium einer Datenverarbeitung zu hinterfragen, ob personenbezogene Daten überhaupt gespeichert werden müssen oder ob dies nicht ggf. entbehrlich ist. Sofern letzteres der Fall ist, ist von einer Speicherung und damit von der Verarbeitung unter allen Umständen abzusehen. Auch der Zugriff auf die gespeicherten Daten unterfällt dem Begriff der Verarbeitung und ist deshalb auf den jeweils erforderlichen Umfang zu beschränken. Gerade für DLT-basierte Technologien stellt sich in besonderem Maße die Frage, ob diese dem Grundsatz der Datensparsamkeit genügen. Hier kommt es entscheidend auf die im Einzelfall gewählte technische Ausgestaltung an.

e) Datenschutz-Folgenabschätzung (DSFA)

Gem. Art. 35 Nr. 1 S. 1 DS-GVO ist von dem Verantwortlichen vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen (Datenschutz-Folgenabschätzung), wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände

[2] Siehe insb. zu Blockchains und Art. 26 DS-GVO: BeckOK Datenschutzrecht/*Spoerr*, Art. 26 DS-GVO Rn. 1 ff., 4a.
[3] BeckOK Datenschutzrecht/*Spoerr*, Art. 26 DS-GVO Rn. 32.
[4] Vgl. BeckOK Datenschutzrecht/*Spoerr*, Art. 26 DS-GVO Rn. 33.

und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Unter Umständen fällt auch der Einsatz der Blockchain/DLT zum Schutz von Ernährung und Logistik hierunter. Aus der *Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist* ergibt sich aus Punkt 4 etwa, dass eine Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen eine solche DSFA erforderlich machen kann, wenn die Verarbeitung umfangreich ist.[5] Soweit im Rahmen eines DLT-Forschungsansatzes beispielsweise Standort- bzw. Bewegungsdaten aufgezeichnet und gespeichert werden, hängt es von deren Umfang ab, ob das Erfordernis für eine DSFA besteht.

f) Unveränderbarkeit

Das bedeutendste datenschutzrechtliche Problem im Rahmen einer Verarbeitung von personenbezogenen Daten innerhalb von Blockchain/DLT stellt die Löschung dar. Das Recht auf Löschung aus Art. 17 DS-GVO ist einer der Grundgedanken des europäischen Datenschutzrechts. Danach hat der Betroffene grds. das Recht, dass die seine Person betreffenden personenbezogenen Daten restlos entfernt werden. Die Unveränderbarkeit der Daten, die aus technischer Sicht eine wesentliche und tragende Eigenschaft der DLT darstellt, soll jedoch gerade die Integrität der Daten gewährleisten. Ein einmal eingetragener Datensatz soll folglich nicht wieder geändert oder gar gelöscht werden können. Dieses tragende Grundprinzip der DLT steht dem Betroffenenrecht diametral entgegen. Diese Problemstellung wird deshalb auch umfassend datenschutzrechtlich diskutiert.

Innerhalb der DLT lässt sich dieses Problem ohne fundamentale Änderung der Struktur einer DLT wohl kaum beheben. Die Lösung muss deshalb prima facie *außerhalb* der DLT erfolgen. Damit dürfen personenbezogene Daten beispielsweise in einer blockchain-basierten DLT nicht in der Blockchain selbst gespeichert werden. Alle personenbezogenen Daten dürften also nur vollständig anonymisiert in die DLT eingebracht werden. Eine bloße Pseudonymisierung dürfte hier regelmäßig nicht ausreichen, da anderenfalls potenziell immer eine Zuordnung möglich

[5] DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.

wäre und auf diese Weise personenbezogene Daten i.S.d. DS-GVO vorlägen (s.o.). Einzig pseudonymisierte Daten, deren Zuordnung *außerhalb* der DLT erfolgt und die somit durch Löschung außerhalb gespeicherter Daten anonymisiert werden können, wären demnach rechtskonform – auch dies wäre aber für den jeweils vorliegenden Einzelfall eingehend zu prüfen. Diese Lösung wird für gewöhnlich, bezogen auch auf Blockchain-DLTs, unter dem Stichwort „Off-Chain Storage" diskutiert und setzt zur Speicherung der personenbezogenen Daten auf herkömmliche zentrale Speicher, wobei innerhalb der DLT damit nur eine Referenz auf diese außerhalb liegenden Daten geschaffen wird. Diese außerhalb liegenden herkömmlichen Datenbanken erlauben damit die Löschung der personenbezogenen Daten, ohne dass dafür in die DLT selbst eingegriffen wird. Die darin enthalten Referenzen würden, im Falle einer Löschung, im Ergebnis auf nicht mehr existente (personenbezogene) Daten verweisen. Die Distributed Ledger müssen also nicht verändert werden, sodass dieser Workaround die DS-GVO-konforme Ausgestaltung einer DLT wäre. Der vorgestellte Ansatz wird jedoch teils kritisch gesehen, da so der Sicherheits- und Transparenzaspekt der Blockchain als Beispiel-DLT ein Stück weit negiert wird, denn schließlich werden die personenbezogenen Daten am Ende doch auf externen herkömmlichen Datenbanken gespeichert, sodass keine vollständige Transparenz mehr dahingehend besteht, wer Zugriff auf die Daten hat.

Juristisch zu untersuchen ist damit letztendlich, ob nicht doch eine DS-GVO-konforme Ausgestaltung der DLT gefunden werden kann, in der für die personenbezogenen Daten nicht zwangsweise auf Off-Chain-Lösungen zurückgegriffen werden muss. Eine ebenfalls diskutierte Möglichkeit bezogen auf Blockchain-DLTs wäre zum Beispiel, die personenbezogenen Daten verschlüsselt direkt in der Blockchain zu speichern, aber auf Antrag oder nach bestimmten Zeitintervallen die Entschlüsselungs-Keys zu löschen, welche nicht selbst in der Blockchain zu speichern sind, sodass die Daten letztendlich zwar nur pseudonymisiert weiter gespeichert werden, aber ohne den zugehörigen Key, sodass dem Grunde nach der Personenbezug nicht mehr hergestellt werden kann. Auch für diesen Fall kann die DS-GVO-Konformität aber nicht im generellen festgestellt werden, sondern ist für jeden Einzelfall rechtlich genau zu prüfen. Zumindest die nationale französische Datenschutzbehörde CNIL hält diese Lösung wohl für DS-GVO-konform, verweist jedoch darauf, dass die Konformität zur DS-GVO noch detailliert überprüft werden muss.[6] Als Argument dafür, dass die Vernichtung des Entschlüsselungs-Keys

[6] https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

als Löschung i.S.d. DS-GVO anzusehen ist, wird unter anderem angeführt, dass verschlüsselte Daten ohne Entschlüsselungs-Key quasi dem Schutzniveau einer Anonymisierung oder tatsächlichen Löschung entsprechen. Auch diese Variante beinhaltet jedoch ein technisches Restrisiko, dass die Daten, auch wenn der tatsächliche Key gelöscht wurde, entschlüsselt werden können. Juristisch besteht hier deshalb zumindest gegenwärtig noch keine zweifelsfreie Einigkeit.

V. Arbeitnehmerschutzrecht

Datenschutzrechtliche Fragen stellen sich für den DLT-Einsatz auch im Arbeitsrecht – gerade hier ist eine Anonymisierung deshalb von besonderer Bedeutung. Soweit gespeicherte Daten Rückschlüsse auf konkrete Arbeitnehmer zulassen, wenn sie etwa die Zeiten oder Routen von Transporten dokumentieren und hieraus deutlich wird, wer diese betreut hat, stehen solche Aufzeichnungen auch in Konflikt mit den Individualinteressen der Arbeitnehmer. Automatisch sind auch deren Betroffenenrechte aus der DS-GVO tangiert. Gerade im Arbeitsrecht tritt erschwerend hinzu, dass erhöhte Anforderungen an die Wirksamkeit von Einwilligungen des Personals zu stellen sind, da dieses infolge des Arbeitnehmerstatus einer eingeschränkten Willensbildung unterliegt – dies gilt vor allem für die Freiwilligkeit der erteilten Einwilligung als Folge des strukturellen Ungleichgewichts zwischen Arbeitnehmer und Arbeitgeber.[7]

Zu denken ist ferner – soweit vorhanden – an eine Beteiligung des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG, wenn technische Einrichtungen eingeführt oder angewendet werden, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Hierbei kommt es – entgegen des Wortlauts – nicht auf eine konkrete Überwachungsabsicht an, die Überwachung kann vielmehr auch bloßer Nebeneffekt sein.[8] Die technische Einrichtung muss also lediglich *objektiv geeignet* sein, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.[9] Eine Erfassung etwa von Produktionsmengen oder Bewegungsdaten dürfte sich dafür regelmäßig eignen.

[7] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DS-GVO Rn. 21; Erwägungsgrund 34 des Kommissionsvorschlags.
[8] BeckOK Arbeitsrecht/*Werner*, § 87 BetrVG, Rn. 92.
[9] BeckOK Arbeitsrecht/*Werner*, § 87 BetrVG, Rn. 92.

VI. Kritische Infrastrukturen (KRITIS)

Seit dem ersten IT-Sicherheitsgesetz (IT-SiG) aus dem Jahr 2015 wurden umfangreiche cybersicherheitsrechtliche Regelungen für die Betreiber von Kritischen Infrastrukturen (KRITS) getroffen. Grds. handelt es sich gem. § 2 Abs. 10 BSIG bei den Sektoren Ernährung und Transport und Verkehr um Kritische Infrastrukturen. Eine zahlenmäßige Konkretisierung findet für einzelne Sektoren und Branchen durch die BSI-KritisV statt. Im Sektor Ernährung sind beispielsweise solche Anlagen der Kritischen Infrastruktur zuzurechnen, die durch Herstellung, Umschlag, etc. eine in Anhang 3 Teil 3 BSI-KritisV bezifferte Menge erreichen oder überschreiten. Diese Menge liegt zurzeit für Speisen bei 434.500 t und für Getränke bei 350.000.000 l. Im Sektor Transport und Verkehr ist die Gütermenge von 17.000.000 t/Jahr einstufungsrelevant. Ab diesem Schwellenwert ist eine Anlage oder ein System zum Betrieb eines Logistikzentrums der Kritischen Infrastruktur zuzurechnen. Davon ausdrücklich umfasst sind auch IT-Systeme.

Das IT-SiG verpflichtet die Betreiber der Kritischen Infrastrukturen u.a. dazu, technische und organisatorische Maßnahmen zu treffen, um eine angemessene IT-Sicherheit zu gewährleisten. Diese Maßnahmen müssen dem *Stand der Technik* entsprechen. Hierbei handelt es sich um einen unbestimmten Rechtsbegriff bzw. um eine Generalklausel, deren nähere Definition vor allem anhand einschlägiger technischer Normen und Standards erfolgt. Die Erfüllung der Anforderungen ist gem. § 8a Abs. 3 BSIG regelmäßig nachzuweisen. Rechtlich gesehen kann die Möglichkeit, durch den Einsatz von DLT Lieferketten nachzuverfolgen, in Zukunft wohl auch zur Sicherung des Standes der Technik beitragen. Auch international wird die Nutzung von DLT und Blockchains im Speziellen als Basis für eine sichere Supply Chain, insbesondere auch unter Compliance Gesichtspunkten für Kritische Infrastrukturen, diskutiert.[10]

VII. Smart Contracts

Smart Contracts sind nicht grds. Verträge im Rechtssinne. Vielmehr umfassen sie oftmals nur automatisierte Ausführungen anhand zuvor festgelegter Regeln nach dem System einer Wenn-dann-Verknüpfung. Sofern tatsächlich aber rechtsgeschäftliche Einigungen abgebildet werden sollen, ergeben sich hieraus ebenfalls juristische Anforderungen und Probleme, so z.B.

[10] Siehe beispielsweise Next Generation Supply Chain Security for Energy Infrastructure and NERC Critical Infrastructure Protection (CIP) Compliance, *Mylrea/Gourisetti* in Journal on Systemics, Cybernetics and Informatics: JSCI Volume 16 Number 6 2019, 22, https://pdfs.semanticscholar.org/9bdf/dd05608a122ec86b96a5af3a2c22666fc72d.pdf.

für den Vertragsschluss. Denkbar ist, dass es zum Abschluss eines Vertrags gänzlich ohne Tätigwerden einer natürlichen Person kommt. Damit ist das wirksame Zustandekommen eines Vertrages, das zwei übereinstimmende Willenserklärungen erfordert, wegen der fehlenden Zuordnung zu natürlichen Personen fraglich.

Aus Entwicklersicht könnte darüber hinaus bereits die Erstellung solcher Smart Contracts rechtliche Schwierigkeiten bereiten. Sofern tatsächlich Verträge im rechtlichen Sinne geschlossen oder abgewickelt werden, können Entwickler mit Blick auf das Gesetz über außergerichtliche Rechtsdienstleistungen (RDG) nur bedingt (alleine) tätig werden. Wenn in konkreten fremden Angelegenheiten eine rechtliche Prüfung des Einzelfalls erfolgt, so handelt es sich um eine Rechtsdienstleistung i.S.d. § 2 Abs. 1 RDG. § 3 RDG statuiert ein grundsätzliches Verbot zur Erbringung solcher Rechtsdienstleistungen, soweit keine ausdrückliche gesetzliche Erlaubnis besteht. Bei der Erstellung eines Smart Contracts ist folglich im Einzelfall zu prüfen, ob dieser schon derart einzelfallbezogen eine rechtliche Prüfung vornimmt (etwa durch das Maß der Berücksichtigung der konkreten Anforderungen und Bedürfnisse), dass es sich um eine Rechtsdienstleistung i.S.d. RDG handelt.

VIII. Vertiefende Literatur

Eschenbruch/Gerstberger: Smart Contracts, NZBau 2018, 3

Heckelmann: Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504

Paulus/Matzke: Smart Contracts und das BGB – Viel Lärm um nichts?, ZfPW 2018, 431

Krupar/Strassemeyer: Datenschutz auf der Blockchain – die Innovationsfeindlichkeit der DS-GVO, in: Tagungsband DSRI-Herbstakademie 2018, S. 343

Kaufhold: Blockchain Technologie im Licht des Risk Based Approach der DS-GVO, in: Tagungsband DSRI-Herbstakademie 2018, S. 397