Universität Bremen*
*EXCELLENT.

NutriSafe – Vorstellung der Projektergebnisse

Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen
Wien, den 11. März 2020

Agenda

I. **Der Rechtsrahmen für den praktischen Einsatz der DLT**
   1. Datenschutz
   2. Arbeitsrecht/Arbeitnehmerdatenschutz
   3. Anforderungen an Kritische Infrastrukturen (KRITIS)
   4. Smart Contracts

II. **Arbeiten an relevanten technischen Normen und Standards**

III. **Entwicklung und Konzeptionierung des juristischen Kompendiums**

Universität Bremen*
*EXCELLENT.

Der Rechtsrahmen für den praktischen Einsatz der DLT I

Stand der Bearbeitung: 03.09.2019

IGMR

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

II. Funktionsweise der DLT

III. Grundlegendes zum Rechtsrahmen

IV. Datenschutz

- a) Begriff des personenbezogenen Datums
- b) Anforderungen an die Erhebung von personenbezogenen Daten
- c) Dezentralität der Datenverarbeitung
- d) Grundsatz der Datenminimierung/Datensparsamkeit
- e) Datenschutz-Folgenabschätzung (DSFA)
- f) Unveränderbarkeit

V. Arbeitnehmerschutzrecht

VI. Kritische Infrastrukturen (KRITIS)

VII. Smart Contracts

Universität Bremen*
*EXCELLENT.

Der Rechtsrahmen für den praktischen Einsatz der DLT II

C811 | Gesetz

	Bezeichnung	Einzelne rechtliche Vorschriften	Technisch	Gesetzesmaterialien, Rechtsprechung und Literatur	Branche
807	Hamburgisches Ausführungsgesetz zum Tiergesundheitsgesetz (AGTierGesG) Vom 15. Dezember 2015	§§ 5; 6 III, IV, V		Zeile 443 - 459	Ernährungswirtschaft
808	Hessisches Ausführungsgesetz zum Tiergesundheitsgesetz	§ 12		Zeile 443 - 459	Ernährungswirtschaft
809	Ausführungsgesetz zum Tiergesundheitsgesetz	§ 6		Zeile 443 - 459	Ernährungswirtschaft
810	Ausführungsgesetz zum Tiergesundheitsgesetz	§ 18		Zeile 443 - 459	Ernährungswirtschaft
811	Gesetz zur Ausführung des Lebensmittel- und Futtermittelgesetzbuches, des Vorläufigen Tabakgesetzes und des Verbraucherinformationsgesetzes im Freistaat Sachsen	§ 12		Zeile 443 - 459	Ernährungswirtschaft
812	Landesjagdgesetz für Sachsen-Anhalt	§ 48b		Zeile 443 - 459	Ernährungswirtschaft
813	Gesetz über die Kammern für Heilberufe Sachsen-Anhalt	§ 5 I Nr. 4		Zeile 443 - 459	Ernährungswirtschaft
814	Gesetz über die Kammern und die Berufsgerichtsbarkeit für die Heilberufe (Heilberufekammergesetz)	§ 3 I Nr. 4, IV		Zeile 443 - 459	Ernährungswirtschaft
815	Landesverordnung zur Durchführung des Landesfischereigesetzes	§ 2		Zeile 443 - 459	Ernährungswirtschaft
816	Thüringer Ausführungsgesetz zum Tiergesundheitsgesetz (Thüringer Tiergesundheitsgesetz)	§ 35		Zeile 443 - 459	Ernährungswirtschaft
817	Thüringer Fischereiverordnung	§§ 17-21		Zeile 443 - 459	Ernährungswirtschaft
818	Thüringer Verordnung zur Durchführung des Weinrechts und zur Übertragung von Ermächtigungen auf dem Gebiet des Weinrechts	§ 22		Zeile 443 - 459	Ernährungswirtschaft
819	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	Art. 17 II; **18; 52**		Zeile 460 - 478	Lebensmittelhandel
820	Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG	Alle, inbes. Art. 11; 17 IV f); 19 I, II; 20 I, II; 24 II b) e) f) g) h) j); 26 d); 36 d; 44 I d), e)		Zeile 460 - 478	Lebensmittelhandel
821					
822	RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union	Alle, insbes. Art. 14-16		Zeile 460 - 478	Lebensmittelhandel

Universität Bremen*
*EXCELLENT.

Der Rechtsrahmen für den praktischen Einsatz der DLT III

§ 8 Abs. 1 Fischseuchenverordnung: Buchführung

„Der Betreiber

1. eines Aquakulturbetriebes hat über

a) alle Zugänge unter Angabe der Daten der Anlieferung, der Fischart, des Durchschnittsgewichts der jeweiligen Fischart, deren Stückzahl oder des Gesamtgewichts, des Herkunftsbetriebes und des Transporteurs (…) Buch zu führen .“

- Durch Blockchain kann die Lieferkette manipulationssicher dokumentiert werden
- Datenaustausch der an der Lieferkette partizipierenden Unternehmen untereinander
- Der Verwaltungsaufwand wird verringert
- Verbraucher können die Lieferkette nachverfolgen

Universität Bremen*
*EXCELLENT.

Der Rechtsrahmen für den praktischen Einsatz der DLT IV

§ 10 Abs. 4 Tierische Lebensmittel-Hygieneverordnung

„1. Wer (als Halter von Schlachttieren) Informationen übermittelt (…) *hat hierüber Nachweise zu führen. Die Nachweise (…) sind in übersichtlicher Weise geordnet und fortlaufend zu führen. Die Nachweise sind vom Zeitpunkt der Übermittlung oder Einholung der Informationen (…) an zwölf Monate lang aufzubewahren (…).“*

- Die Informationen in der Blockchain werden fortlaufend gespeichert
- Die Blockchain speichert Daten zeitlich unbegrenzt

Der Rechtsrahmen für den praktischen Einsatz der DLT V

Art. 18 VO EG 178/2002: Rückverfolgbarkeit

„(1) Die Rückverfolgbarkeit von Lebensmitteln und Futtermitteln, von der Lebensmittelgewinnung dienenden Tieren und allen sonstigen Stoffen, die dazu bestimmt sind oder von denen erwartet werden kann, dass sie in einem Lebensmittel oder Futtermittel verarbeitet werden, ist in allen Produktions-, Verarbeitungs- und Vertriebsstufen sicherzustellen.“

- Dokumentation und Rückverfolgbarkeit relevanter Parameter durch Implementierung von Daten in der Blockchain
- Zugriff auf Daten für Abnehmer gewährleistet Transparenz und Kundenvertrauen
- DLT ermöglicht eine eingriffssichere Buchführung und Sicherheit für den Endverbraucher

Der Rechtsrahmen für den praktischen Einsatz der DLT VI

§ 2 Verordnung über tiefgefrorene Lebensmittel: Anforderungen an das Herstellen und Behandeln

„(4) Nach dem Tiefgefrieren muss die Temperatur bis zur Abgabe an den Verbraucher an allen Punkten des Erzeugnisses ständig bei minus 18 Grad C oder tiefer gehalten werden. Von dieser Temperatur sind folgende Abweichungen nach oben zulässig:

1. beim Versand kurzfristige Schwankungen von höchstens 3 Grad C,

2. beim örtlichen Vertrieb und in den Tiefkühlgeräten des Einzelhandels im Rahmen redlicher Aufbewahrungs- und Vertriebsverfahren Abweichungen von höchstens 3 Grad C.

Dem Verbraucher stehen Anbieter von Gemeinschaftsverpflegung sowie Gewerbetreibende, soweit sie Lebensmittel zum Verbrauch innerhalb ihrer Betriebsstätte beziehen, gleich.“

- Messgeräte können als „Hardware-Oracles“ die gemessenen Temperaturen als Datensätze in die Blockchain einspeisen
- Erleichtert den Nachweis einer Unterbrechung der Kühlkette und somit ggf. die Durchsetzung von Gewährleistungsrechten
- Einsichtnahmemöglichkeit für Behörden erleichtert Kontrollen und Aufklärung von Straftaten nach § 59 Abs. 1 Nr. 21 lit. a LFGB iVm §§ 7, 3, 2 TLMV

Rechtsrahmen I

- Im Hinblick auf DLT/Blockchain für den Ernährungssektor **nur wenige spezifische Vorschriften** mit konkretem Erwartungshorizont
- Rechtsrahmen, in dem sich diese Technologien bewegen, ist deshalb aus allgemeinen (und zahlreichen) 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

Rechtsrahmen II

- **Zentrales Problem** für die Anwendung des Datenschutzrechts: **Personenbeziehbarkeit** der Datenbestände! → Wann besteht die Gefahr des Rückschlusses auf eine konkrete Person? Ab wann liegt tatsächlich ein anonymisiertes Datum vor?
- **Juristische Anforderungen:** Voraussetzungen für die Zulässigkeit der Erhebung, Speicherung und Verarbeitung und ferner die Anforderungen an die Technologie im Hinblick auf den Umgang mit solchen Daten
- Die Anforderung von technisch-organisatorischen Schutzvorkehrungen gilt unabhängig von der Frage, ob in einer betroffenen Einrichtung personenbezogene Daten verarbeitet werden

Datenschutz

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-

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

Universität Bremen*
*EXCELLENT.

Allgemeiner Datenschutz I

Ausgangspunkt – in der DLT zu speichernde Datensätze:

- **Daten aus gesetzlichen Anforderungen** an die Rückverfolgbarkeit von Lebensmitteln (VO EG Nr. 178/2002) und Lebensmittel- und Futtermittelgesetzbuch (LFGB): Lieferanten- und Abnehmerdaten, Daten zur gelieferten Ware
- **Daten zur Qualitätssicherung**, die aus den zwischen einzelnen Verarbeitungsschritten fortwährend durchgeführten Qualitätskontrollen stammen
- **Standortdaten**, z.B. eines Transportfahrzeugs, das mittels GPS erfasst wird

Allgemeiner Datenschutz II

Personenbezug der in der DLT zu speichernden Datensätze:

- **Reine Unternehmensdaten** grds. (-), enthält die Bezeichnung der jur. Person aber den Namen der natürlichen Gesellschafter, so grds. (+), vgl. relevanten Fall der „Urproduktion“ im Primärsektor
- **Standortdaten:** Personenbezug grds. (+), ausreichend, wenn Identifizierung unter Zuhilfenahme von Dienst- oder Einsatzplan erfolgt
- **Qualitätskontrolle:** Daten erlauben Rückschlüsse, wer zu welchem Zeitpunktpunkt für Qualitätskontrolle zuständig war – unabhängig von Pseudonymisierung

Allgemeiner Datenschutz III

Zur Herstellbarkeit des Personenbezugs (Identifizierbarkeit):

- Akteur mit Zugriff auf die Blockchain benötigt idR zur Identifizierung weitere Mittel
- **EG 26 S. 3 DS-GVO:** Zur Beurteilung der Identifizierbarkeit sind alle solche Mittel zu berücksichtigen, die vom Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden → hierzu sind alle objektiven Faktoren wie Kosten, Zeitaufwand und verfügbare Technologie zu berücksichtigen

Frage: Inwieweit ist das Wissen des einen Teilnehmers an der Blockchain auch für den anderen Teilnehmer (rechtlich) relevant?

Allgemeiner Datenschutz III

Zur Herstellbarkeit des Personenbezugs (Identifizierbarkeit):

- **Relativer Ansatz:** Zusatzwissen Dritter ist unbeachtlich
- **Absoluter Ansatz:** Identifizierbarkeit durch beliebigen Dritten reicht aus
- **Vermittelnder Ansatz:** Wissen des Verantwortlichen kann um das Wissen Dritter ergänzt werden, soweit wahrscheinlich ist, dass er sich dieses verschaffen könnte und auch wird → Schwelle aber niedrig!
- **Ergebnis:** Personenbezug der iRv NutriSafe gespeicherten Daten in der Blockchain ist grds. zu bejahen

Allgemeiner Datenschutz IV

Anforderungen an die Rechtmäßigkeit der Datenverarbeitung:

- DS-GVO: Verbotsprinzip mit Erlaubnisvorbehalt
- **Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung:** vgl. VO EG Nr. 178/2002 und LFGB
- **Datenverarbeitung zur Vertragserfüllung:** Gilt insb. für Lieferanten- und Kundendaten
- **Einwilligung:** Insb. dann relevant, wenn weitere Unternehmen/unbeteiligte Dritte Einsicht in das Blockchain-Verzeichnis nehmen können

Allgemeiner Datenschutz V

Dezentralität der Datenverarbeitung in der Blockchain: DS-GVO hat aber eine zentrale Stelle als Verantwortlichen vor Augen

- Bestimmung primärer Verantwortlichkeit erforderlich
- Lösung ggf. über Art. 26 DS-GVO (**Joint Controllership**) möglich: Wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, sind sie gemeinsam verantwortlich
- Dabei haben die Netzwerkbeteiligten eine **transparente Vereinbarung** zu schließen, die die Verantwortlichkeiten klar regelt
- Auch müssen Regelungen vorgesehen werden, auf welche Weise die **datenschutzrechtlichen Betroffenenrechte (!)** ausgeübt werden können

Allgemeiner Datenschutz VI

- **Grundsatz der Datenminimierung/Datensparsamkeit:** 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

- **Datenschutz-Folgenabschätzung (DSFA):** Ist durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat → für DLT grds. der Fall, insb. dann, wenn Standort- und Bewegungsdaten aufgezeichnet werden

Allgemeiner Datenschutz VII

Unveränderbarkeit der Daten:

- **Recht auf Löschung aus Art. 17 DS-GVO** ist einer der Grundgedanken des europäischen Datenschutzrechts → DLT aber gerade: Unveränderbarkeit der Datensätze!
- Umfassende datenschutzrechtliche Diskussion
- Innerhalb der DLT lässt sich dieses Problem ohne fundamentale Änderung der Struktur einer DLT wohl kaum beheben → Lösung muss deshalb prima facie ***außerhalb* der DLT** erfolgen
- Alle personenbezogenen Daten dürften also nur vollständig **anonymisiert** in die DLT eingebracht werden
- Aber pseudonymisierte Daten, deren Zuordnung *außerhalb* der DLT erfolgt und die somit durch Löschung außerhalb gespeicherter Daten anonymisiert werden können, wären demnach rechtskonform **(„Off-Chain Storage“**)
- Weitere Möglichkeit: Personenbezogene Daten werden verschlüsselt direkt in der Blockchain gespeichert, aber auf Antrag oder nach bestimmten Zeitintervallen sind die **Entschlüsselungs-Keys zu löschen**

Arbeitnehmerdatenschutz I

- 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**
- Ggf. 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**
- **Extensive Auslegung des BAG:** Mitbestimmungspflichtigkeit besteht auch, wenn die technische Einrichtung nur *geeignet* ist, die Leistung zu überwachen

Arbeitnehmerdatenschutz II

- **Beispiele für mitbestimmungspflichtige Einrichtungen:**
  - GPS-Tracking von LKW einer Spedition zur Bewertung der Wirtschaftlichkeit der Fahrweise
  - Updates von Software, die zur Leistungsüberwachung geeignet ist, unabhängig davon, ob das Update sich auf diese Funktion bezieht
- In der Praxis werden oft **Rahmenvereinbarungen** ausgehandelt, die Fragen der Mitbestimmung zusammenfassend regeln. So muss nicht über jede technische Einrichtung einzeln verhandelt werden

Anforderungen an Kritische Infrastrukturen (KRITIS) I

- **Ernährungssektor** und **Transportsektor** grds. KRITIS
- Soweit Schwellenwerte nach BSI-KritisV überschritten, verpflichtet BSIG zu **TOM** nach „Stand der Technik“ und IT-sicherheitsbezogenen **Meldungen**
- Einzelfallbetrachtung richtet sich nach **BSI-KritisV**

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Lebensmittelversorgung**		
1.1	Lebensmittelherstellung und -behandlung		
1.1.1	Anlage zur Herstellung von Lebensmitteln	Menge der hergestellten Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.1.2	Anlage zur Behandlung von Lebensmitteln	Menge der behandelten Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.1.3	Anlage oder System zur Distribution von Lebensmitteln	Menge der umgeschlagenen Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.1.4	Anlage oder System zur zentralen standortübergreifenden Steuerung	Gesamtmenge der jeweils hergestellten, behandelten oder umgeschlagenen Lebensmittel der gesteuerten Anlagen in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l
1.2	Lebensmittelhandel		
1.2.1	Anlage zur Behandlung von Lebensmitteln	Menge der behandelten Lebensmittel in t/Jahr oder l/Jahr	Speisen: 434 500 t oder Getränke: 350 Millionen l

Anforderungen an Kritische Infrastrukturen (KRITIS) II

Fourteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection

SRI International
1100 Wilson Boulevard, Suite 2800 (28th Floor)
Arlington, Virginia 22209
March 16-17, 2020

2.2 European and German Legislation on Critical Infrastructure Protection

Based primarily on the European and German political strategies for the protection of critical infrastructures, various laws have been passed in recent years, which also means that there is no uniform law for the implementation of cyber security. This is also a challenge for those companies addressed by the laws. As far as IT security-specific legislation in the EU and in Germany is concerned, the following legal sources can currently be used as key drivers of corporate information security:

- the EU Network and Information Security Directive from 2016 (EU NIS Directive)
- the EU Cybersecurity Regulation from 2019 (EU CSA)
- the German IT Security Act 2015 (IT-SiG) including the BSI Critical Infrastructure Ordinance (BSI-KritisV, published in two stages in 2016 and 2017 respectively)
- the draft version of the 2nd German IT Security Act (IT-SiG 2.0, 2019)

The IT security-specific regulations, which were established by the German IT-SiG, essentially address the operators of critical infrastructures. These

Universität Bremen*
*EXCELLENT.

Smart Contracts I

- 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, z.B. im Hinblick auf die **Verantwortlichkeit** für kausal eingetretene Schäden
- Aus **Entwicklersicht** könnte darüber hinaus bereits die Erstellung solcher Smart Contracts rechtliche Schwierigkeiten bereiten:

Smart Contracts II

- Sofern tatsächlich Verträge im rechtlichen Sinne geschlossen oder abgewickelt werden, können Entwickler mit Blick auf das Gesetz über **außergerichtliche Rechtsdienstleistungen** (RDG) nur bedingt (allein) tätig werden
- Wenn in konkreten fremden Angelegenheiten eine rechtliche Prüfung des Einzelfalls erfolgt, so handelt es sich um eine **Rechtsdienstleistung** iSd § 2 Abs. 1 RDG
- § 3 RDG statuiert ein **grundsätzliches Verbot** zur Erbringung solcher Rechtsdienstleistungen

Smart Contracts III

Beispiel: Ernteausfallversicherungen

- Registrierung des Erntegrundstücks des Versicherungsnehmers in einem dem Smart Contract anhängigen Grundstücksverzeichnis
- Einpflegen eines zuvor vereinbarten Wetterereignisses in den Smart Contract (zum Beispiel Hagelstürme)
- Erfassen des Wettereignisses durch sog. „Oracles“ und automatische Auszahlung der Versicherungssumme

Universität Bremen*
*EXCELLENT.

Smart Contracts IV

Beispiel: Ernteausfallversicherungen – Einsatz von Oracles

- An den Smart Contract gekoppelte „Wissensquellen“, die den Zustand in der realen Welt wiedergeben können
- In Form von Datenbanken, Sensoren aber auch realen Personen, die Überprüfungen von Tatsachen vornehmen können
- Anhängen von Daten an die Blockchain, die den Eintritt der vereinbarten Bedingungen bestätigen und die Grundlage der zugehörigen „Handlungen“ darstellen
- Z.B. Erfassung eines Hagelsturms im Bereich eines verzeichneten und versicherten Grundstückes

Smart Contracts V

Beispiel: Ernteausfallversicherungen – Funktion der Beweisfindung und -sicherung

- Dezentralisierte und manipulationsfeste Sicherung der durch die „Oracles“ bereitgestellten Daten
- Erleichterung des Beweisantritts im Streitfall
- Eintritt des Versicherungsfalls, Geltendmachung von Gewährleistungsrechten in der „Food Supply Chain“, Beweis von sonstigen Pflichtverletzungen
- Z.B. im Sinne eines „elektronischen Dokuments“ gemäß § 371 ZPO (Beweis durch Augenschein)

Arbeiten an relevanten technischen Normen und Standards

	B	C	D	E	F	I	J	L	P	Q
1	Vorsch	numm	Ausgab	Name	Name E	ICS-Klass	Thema	Sektor	Zitiert	Link
302	IEC	TS 62579	2010-05-0(	Multimec	Multimedia	35.160, 35.2	Multimedia	Informationstech	#	https://(
303	IEC	TR 63069	2019-05-0(	Prozess-L	Industrial-p	13.110, 25.0	Industrielle	Informationstech	IEC 61508-1	https://#
304	IEC	2443-1-1	2009-07-0(	|	Industrial c	25.040.40, 3	Industrielle	Informationstech	IEC 62264-1	https://#
305	DIN EN IE	0802-4-1	2018-10-0(	IT-Sicherh	Security for	25.040.40, 3	Industrielle	Informationstech	DIN EN 615(	https://#
306	IEC	2443-4-2	2019-02-0(	Kommuni	Security for	25.040.40, 3	Industrielle	Informationstech	IEC/TS 6244	https://#
307	IEC	2443-2-1	2010-11-0(	Industriel	Industrial c	25.040.40, 3	Industrielle	Informationstech	IEC/TS 6244	https://#
308	IEC	2443-3-3	2013-08-0(	Industriel	Industrial c	25.040.40, 3	Industrielle	Informationstech	IEC/TS 6244	https://(
309	IEC	2443-2-4	2015-06-0(	IT-Sicherh	Security for	25.040.40, 3	Industrielle	Informationstech	#	https://(
310	ISO	26430-3	2008-07-0(	Digitales	Digital cine	35.040.40, 3	Digitales Ki	Medien und Kult	FIPS 197 (20	https://#
311	ISO	26430-4	2009-12-0(	Digitales	Digital cine	35.040.40, 3	Digitales Ki	Medien und Kult	IETF RFC 21	https://#
312	ISO	26430-5	2009-12-0(	Digitales	Digital cine	35.040.40, 3	Digitales Ki	Medien und Kult	IETF RFC 22	https://#
313	ISO	26430-6	2009-12-0(	Digitales	Digital cine	35.040.40, 3	Digitales Ki	Medien und Kult	SMPTE 336M	https://#
314	ISO	26430-9	2009-12-0(	Digitales	Digital cine	35.040.40, 3	Digitales Ki	Medien und Kult	IEEE 1003.1	https://#
315	DIN EN IS	24534-4	2011-10-0(	Automatische Identif		35.240.60, 4	Automatisc	Transport und Ve	EN 12834 (2	https://#
316	DIN EN IS	24978	2011-10-0(	Intelligen	Intelligent	35.240.60	Intelligente	Transport und Ve	ANSI X 3.38	https://#
317	ISO	20214	2015-08-0(	Daten- ur	Space data	49.140	Luft- und Ra	Transport und Ve	#	https://#
318	DIN EN	16495	2014-05-0(	Flugverke	Air Traffic M	03.220.50, 3	Luftfahrt	Transport und Ve	ICAO AN 17	https://#
319	DIN	0831-102	2013-12-0(	Elektrisch	Electric sigr	93.100, RW3	Schienenve	Transport und Ve	DIN EN 5012	https://#
320	DIN	0831-104	2015-10-0(	Elektrisch	Electric sigr	35.240.60, 9	Schienenve	Transport und Ve	DIN EN 5012	https://#
321	DIN EN IE	1162-460	2019-02-0(	Navigatio	Maritime n	47.020.70	Schifffahrt	Transport und Ve	IEC 60812 (2	https://#
322	DIN ISO	9735-5	2004-01-0(	Elektroni	Electronic c	35.240.63	Datenausta	Transport und Ve	DIN ISO 973	https://#
323	DIN ISO	9735-6	2004-01-0(	Elektroni	Electronic c	35.240.63	Datenausta	Transport und Ve	DIN ISO 973	https://#
324	DIN ISO	9735-7	2004-01-0(	Elektroni	Electronic c	35.240.63	Datenausta	Transport und Ve	DIN ISO 973	https://#
325	DIN EN	419231	2019-11-0(	Schutzpro	Protection	35.030, 35.0	Vertrauens	Informationstech	EN 319421 V	https://#

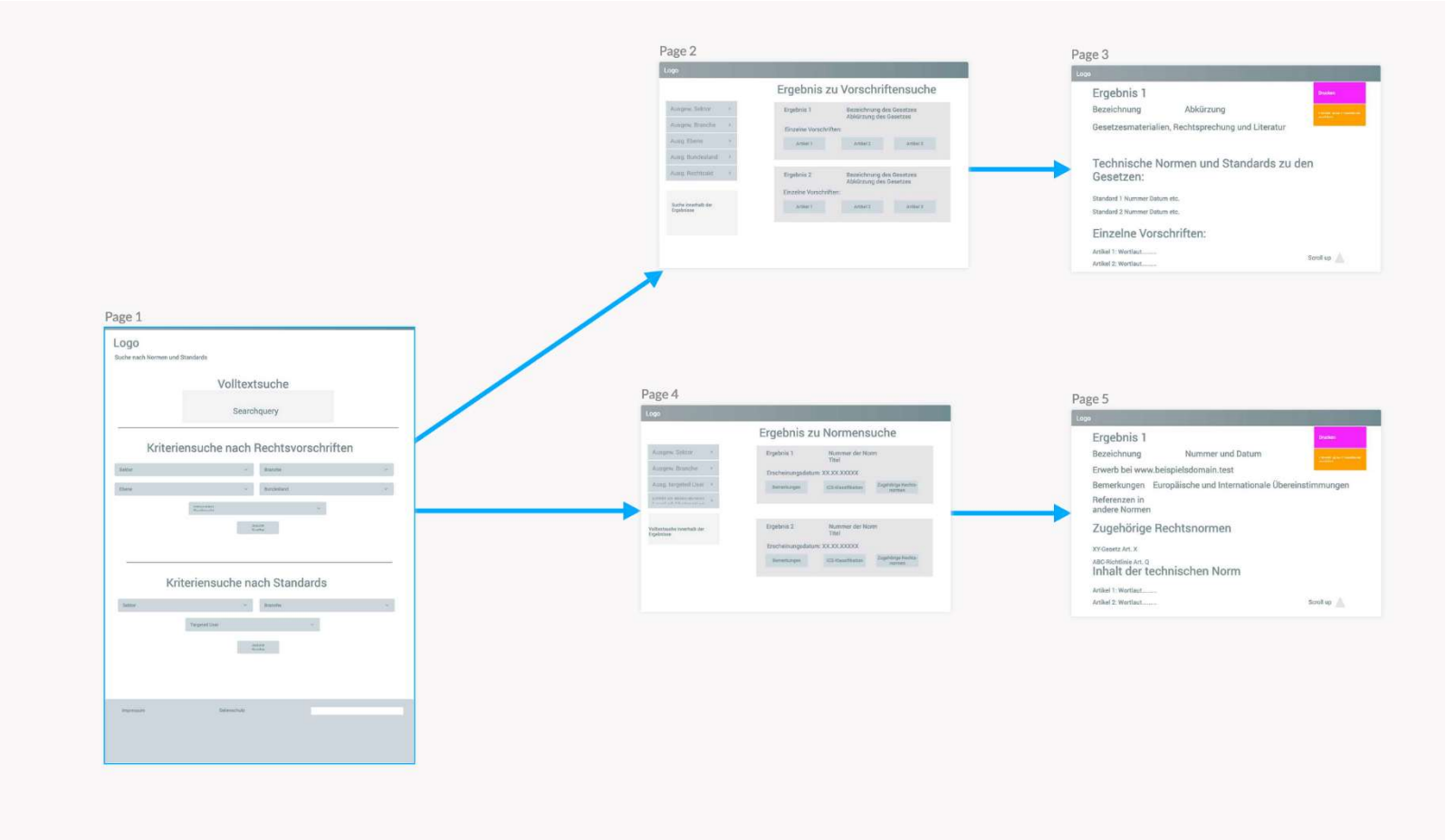
Universität Bremen*
*EXCELLENT.

Arbeiten an relevanten technischen Normen und Standards

Relevante Beispiele:

- **DIN ISO 10008 - Qualitätsmanagement - Kundenzufriedenheit - Leitfaden für den elektronischen Geschäftsverkehr zwischen Unternehmen und Verbrauchern:** Anleitung für Organisationen zur Planung, Gestaltung, Entwicklung, Umsetzung, Aufrechterhaltung und Verbesserung eines wirksamen und effizienten Systems für den elektronischen Geschäftsverkehr zwischen Unternehmen und Verbrauchern (en: business-to-consumer electronic commerce transactions, B2C ECT). Ein solches System kann Verbraucher und Organisationen bei allen Aspekten des elektronischen Geschäftsverkehrs unterstützen und dabei eine Grundlage für Verbraucher schaffen, zunehmendes Vertrauen in den elektronischen Geschäftsverkehr zu gewinnen
- **DIN SPEC 3104 - Blockchain-basierte Datenvalidierung:** Diese DIN SPEC legt den technischen Rahmen und die Funktionen der Blockchain-Validierungssoftware für Blockchain-Validierungsprozesse fest. Insbesondere werden Anforderungen und Bewertungskriterien für den Nachweis der Korrektheit der Blockchain und funktionale Aspekte des Timestamping der Blockchain bereitgestellt
- **ISO/IEC 27036:2013 - Informationstechnik - Sicherheitstechniken - Informationssicherheit für Lieferantenbeziehungen:** Mehrteilige Norm, die eine Anleitung zur Bewertung und Behandlung von Informationsrisiken beim Erwerb von Waren und Dienstleistungen von Lieferanten bietet

Entwicklung und Konzeptionierung des juristischen Kompendiums



Universität Bremen*
*EXCELLENT.

Entwicklung und Konzeptionierung des juristischen Kompendiums

Ergebnis zu Vorschriftensuche (Treffer 32)

Ausgew. Sektor >

Ausgew. Branche >

Ausgew. Ebene >

Ausgew. Bundesland >

Ausgew. Rechtsakt >

Suche innerhalb der Ergebnisse

Volltextsuche

Transnational **Branche: Logistik**

Ergebnis 1

RICHTLINIE 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG
RL 2014/53/EU

Einzelne Vorschriften

Art. 3 I a, 3 III e; 9 II; 10 I, V; 40 I; 42 I

Transnational **Branche: Logistik**

Ergebnis 2

Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
VO Nr. 910/2014

Einzelne Vorschriften

Alle, inbes. Art. 11; 17 IV f); 19 I, II; 20 I, II; 24 II b) e) f) g) h) j); 26 d); 36 d; Art. 44 I d), e)

Transnational **Branche: Logistik**

Universität Bremen*
*EXCELLENT.

Entwicklung und Konzeptionierung des juristischen Kompendiums

Ergebnis zu Vorschriftensuche (Treffer 79)

Ausgew. Sektor >

Ausgew. Branche >

Ausgew. Ebene >

Ausgew. Bundesland >

Ausgew. Rechtsakt >

Suche innerhalb der Ergebnisse

Volltextsuche

Bundesrecht — **Branche: Ernährungswirtschaft**

Ergebnis 21 — IT Sicherheitsgesetz 2.0 **IT SiG 2.0**

Einzelne Vorschriften

Alle

Bundesrecht — **Branche: Ernährungswirtschaft**

Ergebnis 22 — Gesetz zum Schutz von Geschäftsgeheimnissen **GeschGehG**

Einzelne Vorschriften

§§ 1; 4; 7; 23

Bundesrecht — **Branche: Ernährungswirtschaft**

Ergebnis 23 — Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz **BSI-KritisV**

Universität Bremen*
*EXCELLENT.

Universität Bremen*
*EXCELLENT.

Vielen Dank für die Aufmerksamkeit

Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen
Universitätsallee GW1
28359 Bremen
Tel.: +49 421 218 66049
E-Mail: kipker@uni-bremen.de